Emory Bankruptcy Developments Journal

Volume 34
Issue 2 *The Fifteenth Annual Emory Bankruptcy Developments Journal Symposium*

2018

Maximizing the Value of Privacy through Judicial Discretion

Daniel Brian Tan

MAXIMIZING THE VALUE OF PRIVACY THROUGH JUDICIAL DISCRETION

ABSTRACT

Bankruptcy aims to provide maximum redress to creditors. In corporate bankruptcies, legislation and regulation encourage the de-identification of consumer information and the restriction of sales to a limited pool of qualified purchasers operating in a similar industry. Judicial discretion is used to transfer privity from a debtor to a qualified purchaser. Both de-identification and the qualified purchaser requirement reduce consumer data values in bankruptcy and provide only a thin veil of protection. With decreased consumer data values, companies face reduced incentives to secure the data they hold, since tort law requires a recognized harm before it can provide a remedy.

To avoid contravening the aim of bankruptcy and providing minimal protections to consumer privacy, judicial discretion should be used to alter not only the privity among parties but also the terms of purchase in bankruptcy. If purchasers are required to accept a minimum value of tortious liability for failing to secure data, then the amount they are willing to spend on data security will increase. As the security of data increases, its market value will likely follow. This treatment better serves the aims of bankruptcy by maximizing redress to creditors and better serves legislative intent by fostering consumer privacy.

INTRODUCTION

Each year, companies collect ever-increasing amounts of consumer data. As the amount of data possessed by companies increases, the risk of harm associated with a breach of consumer confidentiality grows in kind.[1] Consumer data is collected to provide efficient and targeted services, but companies do not employ adequate security measures to protect the data they have collected.[2]

---

[1] *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Opening Remarks at Fed. Trade Comm'n PrivacyCon 2017, 2 (Jan. 12, 2017); Nancy S. Kim, *Contract's Adaptation and the Online Bargain*, 79 U. CIN. L. REV. 1323, 1341–43, 1349–50, 1355–56 (2011) (criticizing "hook" provisions in online user agreements that authorize the collection, retention, and commercialization of user data); FED TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 2 (Mar. 2012) [hereinafter PRIVACY REPORT].

[2] *See* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1063 (2009) ("Personal information flows are necessary for the functioning of modern economies and are often beneficial to consumers (data subjects), first parties (data holders), and third party companies (data brokers). Consumers benefit from transactions involving their personal

Increased risk of harm is heavily correlated with how many records an entity possesses and the number of compromised records in data breaches increases each year.[3] In 2005, 32,000 private information records were revealed in the George Mason University breach, which is minuscule compared to the massive Yahoo breach of 1.5 billion records in 2016.[4] In 2017, the Equifax data breach demonstrated how a smaller number of records can potentiate severe harms.[5]

Privacy is not generally a concern of bankruptcy law, but it often becomes one when consumer data is sold in corporate bankruptcies. Whether data is liquidated in chapter 7 or leased and sold in chapter 11 plans, corporate filings consolidate large stores of data, which exacerbates the threat to privacy. One of bankruptcy's primary aims is to maximize redress to creditors, but when that redress involves consumer data, courts must weigh creditors' financial interests against consumers' privacy concerns.[6]

Judicial discretion allows bankruptcy courts to balance those interests.[7] In an effort to maximize efficiency and produce equitable results, courts often exercise discretion to authorize the sale of consumer data in bankruptcy. These sales may contradict express company promises that collected data will not be sold.[8] Although courts claim that these distributions help repay creditors while

---

data due to easier access to credit and insurance, customization, and personalization."); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L.REV. 1 (2003); Ramirez, *supra* note 1.

[3] *See* Simson L. Garinkel, NAT'L INST. STANDARDS AND TECH., DE-IDENTIFICATION OF PERSONAL INFORMATION, NIST INTERNAL REPORT 8053 10-14 (October 2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf; Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCI. MAG. 536, 536–38 (2015).

[4] *See* Lazaro Gamio & Chris Alcantara, *How Data Breaches Grew to Massive Proportions in 11 Years*, WASH. POST, Dec. 14, 2016, *available at* https://www.washingtonpost.com/graphics/business/the-scale-of-large-hacks/; Ashley Rodriguez, *How Much Were Yahoo's Massive Breaches Worth? About $350 Million and More Future Headaches*, QUARTZ (Feb. 21, 2017), https://qz.com/912055/verizon-values-yahoos-data-breaches-at-350m-plus-future-headaches/.

[5] Although the information is not conclusive at the time of writing, current estimates intimate that 143 million people may have been affected by the data breach. This means that up to sixty percent of Americans over the age of 18 may have had very sensitive compromised. Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N: CONSUMER INFO. BLOG (Sep. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do; *QuickFacts* Table, U.S. Census Bureau, https://www.census.gov/quickfacts/fact/table/US/PST045216. (last visited Jan. 12, 2018).

[6] 1 COLLIER ON BANKRUPTCY ¶ 1.01[1] (Alan N. Resnick & Henry J. Sommer eds., 16th ed.).

[7] 11 U.S.C. § 105 (2012) ("The court may issue any order, process, or judgment that is necessary or appropriate to carry out the provisions of this title").

[8] *See* Letter from David Vladeck, Director, Fed. Trade Comm'n Bureau of Consumer Prot. to Michael Baxter and Yaron Dori (September 14, 2011) [hereinafter Vladeck Letter to Baxter], *available at* https://www.ftc.gov/news-events/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders; Statement of Commissioner Sheila F. Anthony, Toysmart.com, No. X00-0075, No. 00-13995 (CJK) (D. Mass. Jul. 21, 2000) [hereinafter Anthony Statement], https://www.ftc.gov/sites/default/files/documents/

protecting consumer privacy, data is usually sold for nominal amounts and consumer privacy protections are routinely outdated.[9] As the amount of data collected increases, the concern for consumer privacy must likewise increase, or the law will fail to both repay creditors and protect consumers.[10]

The 2015 RadioShack bankruptcy presents a good example of the way the law currently addresses consumer privacy issues in bankruptcy.[11] RadioShack sold its intellectual property assets, including its trademarks and the personally identifiable information (PII) of 117 million customers.[12] The question of whether RadioShack could sell customer PII became a point of contention for numerous parties, including RadioShack customers, multiple state attorneys general, the Federal Trade Commission (FTC), Apple, Verizon Wireless (Verizon), and AT&T.[13] On RadioShack's petition date, its privacy policy

---

cases/toysmartanthonystatement.htm. *But see* Statement of Commissioner Mozelle W. Thompson, Toysmart.com, No. X00-0075, No. 00-13995 (CJK) (D. Mass. Jul. 21, 2000) [hereinafter Thompson statement] (arguing that the proposed sale of consumer data was not inconsistent with Toysmart's privacy policy), https://www.ftc.gov/sites/default/files/documents/cases/toysamrtthompsonstatement.htm.

[9] In light of the bankruptcy law's stated aims, the rise in consumer data breaches and the minimal valuation of data asset distributions provide evidence of inadequate legal treatment. Conservative estimates suggest 25 major data breaches from businesses in 2005. Those totals rose by an average of 141.23 percent each year until 2016, despite government efforts to deter and prevent data breaches. *Compare* Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA) of 2005, Pub. L. No. 109-8, § 232 §§ 231–34, 110 Stat. 23 (addressing the perceived threats to privacy from the collection and distribution of consumer information, and trying to prevent harm from occurring), *and* Gramm-Leach-Bliley Act, Pub. L. No. 106-102 §§ 501–27, 113 Stat. 1338 (1999) (addressing how banks collect, store, and distribute information to prevent harm), *and* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191 § 221, 110 Stat. 1936 (providing safeguards for medical information) *with* IDENTITY THEFT RESOURCE CENTER, ITRC BREACH STATISTICS 2005–2016 (2017), http://www.idtheftcenter.org/images/breach/2016/Overview2005to2016 Finalv2.pdf (showing data breaches and the harm to consumer privacy despite attempts at prevention). *See, e.g.*, *supra* note 8; Letter from Jessica Rich, Director, Fed. Trade Comm'n Bureau of Consumer Prot. to Elise Frejka (May 16, 2015) [hereinafter Rich Letter], *available at* https://www.ftc.gov/system/files/documents/public_ statements/643291/150518radioshackletter.pdf.

[10] There is a common and growing need to review, address, and manage the collection of consumer privacy. *See*, *e.g.*, Ramirez, *supra* note 1 ("Experts estimate that, by the year 2020, there will be a 4,300 percent annual growth in the amount of data that is collected"). As is common with many goods-turned-commodities, there will be those who harvest, refine, or trade in a desired commodity. *See*, *e.g.*, ACXIOM, 2016 ANNUAL REPORT 13 (2016), http://files.shareholder.com/downloads/ACXM/3857056437x0x897585/1A5C33C7-9C80-4621-8B3E-15F7D2C86D5B/ACXM_Annual_Report_FINAL_RRD_Printers_Proof_6-17-16_.pdf ("We offer multi-sourced insight into approximately 700 million consumers.").

[11] *See* Rich Letter, *supra* note 9. On the RadioShack bankruptcy, *see generally* Alan Wolf, *RadioShack: A Brief History of Time,* TWICE (Feb. 16, 2015), http://www.twice.com/news/retail/radioshack-brief-history-time/56040.

[12] Marshall J. Hogan, *Customer Data Sale in Bankruptcy: Lessons from RadioShack*, LAW360 (July 15, 2015, 2:03 PM EDT), https://www.law360.com/articles/679550/customer-data-sale-in-bankruptcy-lessons-from-radioshack.

[13] Cara Salvatore, *RadioShack Gets OK for Data Sale Deal with Verizon, AT&T*, LAW360 (Jun. 9, 2015, 7:46 PM EDT), https://www.law360.com/articles/665356/radioshack-gets-ok-for-data-sale-deal-with-verizon-at-t; Certification of Counsel Regarding Interim Order Approving Interim Stipulation for Implementation of

defined PII and explained how it would be handled.[14] The policy included an express promise that RadioShack "will not sell or rent [consumer] personally identifiable information to anyone at any time."[15] Reinforcing this promise, the policy also proclaimed, "We pride ourselves on not selling our private mailing list."[16] In light of these promises, it seems intuitive that the court would prevent the sale of the PII, yet the ultimate approval of the sale shows otherwise.

Here, state attorneys general, attempting to mitigate potential privacy harms, objected to the sale of PII.[17] One of their concerns was how many data points, or pieces of information, these records contained.[18] In RadioShack's settlement, it agreed to reduce the twenty-one-point data set of customer information to seven, removing such information as phone numbers and limiting which e-mail addresses were sold.[19] Although the settlement was deemed a success, enhancements in modern technology enable re-identification and targeting based on fewer data points.[20] Therefore, the reduction from twenty-one to seven points did little to deter future breaches.

Protocols with Verizon and AT&T in Connection with the Transfer of Customer Data to General Wireless, *In re* Radioshack, No. 15-10197 (BLS) (Bankr. D. Del. 2015), https://consumermediallc.files.wordpress.com/2015/06/m042115274439.pdf; John Ribeiro, *25 U.S. states oppose sale of RadioShack's customer data*, PCWORLD (Mar. 26, 2015, 5:40 AM).

[14] Rich Letter, *supra* note 9.

[15] "Personally identifiable information may include information that you provide to us by requesting information, when registering for special offers or programs or when you buy products online. This may include your name, address (including billing and shipping addresses), telephone number, e-mail address, organization, city, state and zip code. We may use this information to process and ship orders, to contact you about the status of your order, to contact you with answers to your questions, or to provide information about new and exciting products, services, promotions and corporate-related information. We may use mailings, telephone calls and e-mail to contact you . . . . We will not sell or rent your personally identifiable information to anyone at any time." *Id*. at 2 (quoting RadioShack's then-current privacy policy). Since at least 2004, the privacy policy had specifically claimed that "[RadioShack would] not sell or rent [customers'] personally identifiable information to anyone at any time." *Id*. at 2, n.5.

[16] *See id*. at 3 (citing RadioShack's privacy policy from 2014).

[17] Ribiero, *supra* note 13.

[18] State of Texas's Limited Objection to Sale of Personally Identifiable Information of One Hundred Seventeen Million Consumers, *In re* RadioShack Corp., 2015 Bankr. LEXIS 4541 (Bankr. D. Del. 2015), https://cdn.arstechnica.net/wp-content/uploads/2015/03/1393.pdf.

[19] Among the concessions, RadioShack limited the e-mail addresses sold to those active within two years of petition. Press Release, Eric T. Schneiderman, N.Y. State Attorney Gen., A.G. Schneiderman Announces Agreement to Protect Consumer Data in RadioShack Bankruptcy (May 20, 2015), https://ag.ny.gov/press-release/ag-schneiderman-announces-agreement-protect-consumer-data-radioshack-bankruptcy.

[20] Although it was not stated as a primary factor, it seemed one concern was that of consumers being contacted without consent. The FTC readily admits that modern technology makes it difficult to circumvent these concerns. Bikram Bandy, *Your Top 5 Questions about Unwanted Calls and the National Do Not Call Registry,* FED. TRADE COMM'N: CONSUMER INFO. BLOG (Mar. 9, 2015), https://www.consumer.ftc.gov/blog/your-top-5-questions-about-unwanted-calls-and-national-do-not-call-registry ("Current technology makes it easy for scammers to fake or 'spoof' caller ID information, so the number you reported in your complaint

Further, RadioShack collected consumer information pursuant to its privacy policy when it sold products and services, including those provided by Verizon, Apple, and AT&T.[21] When RadioShack filed for bankruptcy and offered to sell customer information, all three companies objected to the sale of customer information involving their products or services.[22] Verizon and AT&T's objections were granted, while customers who purchased Apple products through RadioShack saw their information sold.[23] This disparate treatment raised two questions: What discretionary powers do bankruptcy courts have to change, ignore, or enforce privacy policy terms? What factors does the law consider when deciding how to handle these sales?

The court followed the FTC's recommendations to impose four requirements: first, that PII not be sold as a stand-alone asset; second, that the buyer be a qualified purchaser engaged in the same line of business as the seller; third, that the buyer agree to honor privacy policy terms; and fourth, that the privacy policy terms would be altered only with the express consent of customers.[24] These standards are not unique to *In re RadioShack*, and, in each circumstance, they are aimed at protecting consumer privacy while maximizing repayment to creditors. Yet, here and elsewhere, they might accomplish neither.

While some have advocated addressing the issue legislatively,[25] this Comment argues that, to protect consumer data while providing redress to creditors, bankruptcy courts should expand the use of judicial discretion in both chapter 7 and chapter 11 corporate bankruptcy proceedings to consider the future value of consumer data when altering contract terms. This expanded use of discretion should establish clear liability values for consumer data breaches, expand the scope of what constitutes a qualified purchaser, and order the destruction of all data not sold before the conclusion of the proceedings.

Company incentives to secure data involve an analysis that weighs the cost of securing the data against the costs that would result from a data breach. Bankruptcy courts should perform three market manipulations to increase

---

probably isn't real. Without more information, it's difficult for us to identify the actual caller. Nonetheless, the FTC analyzes complaint data to identify illegal callers based on calling patterns. The agency also is pursuing a variety of technology-based solutions to combat illegal calls and practices.").

[21] Salvatore, *supra* note 13; Certification of Counsel, *supra* note 13; Ribiero, *supra* note 13.

[22] Salvatore, *supra* note 13.

[23] Certification of Counsel, *supra* note 13; Salvatore, *supra* note 13.

[24] Buyer had to agree to be bound by the privacy policy terms that governed the PII when it was acquired. Rich Letter, *supra* note 9, at 5.

[25] *See* Kayla Siam, *Coming to a Retailer Near You: Consumer Privacy Protection in Retail Bankruptcies*, 33 EMORY BANKR. DEV. J. 487 (2017).

security for consumer data. First, increasing the costs incurred by data breaches would increase the incentive to secure data, which in turn would strengthen consumer data values. Second, expanding the number of qualified purchasers would foster competition among buyers. Third, destroying unsold data would preclude later purchases by those unwilling to protect it and would decrease the available supply. These market manipulations of the supply-demand curve would increase the value of data and thus result in greater redress to creditors. At the same time, an increased incentive to secure consumer data would likely produce beneficial externalities, such as increased consumer awareness of privacy concerns.

This Comment will begin by demonstrating how the organic development of the law has failed to keep pace with rapid technological advancements. Throughout the discussion, this Comment will establish how the law balances consumer privacy concerns with economic interests in legislation, regulation, and jurisprudence. The Comment will then discuss the extent to which bankruptcy courts can alter contract terms through judicial discretion. Finally, the Comment will conclude by offering a solution to protect privacy while increasing redress to creditors by changing how bankruptcy courts use judicial discretion.

I. PRIVACY OUTPACED BY TECHNOLOGY

The legal system generally treats privacy less as an entitlement to be positively asserted than as a right whose violation opens the door to redress. In fact, privacy originated as a value to be preserved through negative rights that developed organically throughout history.[26] Over time, ex ante prohibitions were introduced to guard citizens from unconstitutional invasions by the government, while ex post remedies compensated victims of privacy harms.[27] Even today, there is no standard treatment of privacy rights despite the growing need.[28]

---

[26] *See, e.g.*, William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); RUTH MACKAY, THE BAKER WHO PRETENDED TO BE KING OF PORTUGAL (2012) (in feudal times, Gabriel de Espinosa was sentenced to death for impersonating the late King Sebastian of Portugal); Ross A. Thompson, *Vulnerability in Research: A Developmental Perspective on Research Risk*, 1991 ANNUAL PROGRESS IN CHILD PSYCHIATRY AND CHILD DEV. 119, 135 (Stella Chess & Margaret E. Hertzig eds., 1991) (positing that privacy is a step in self-identity and "[p]rivacy interests and concerns increase and become more differentiated as children mature, and broaden from an initial focus on physical and possessional privacy to include concerns with informational privacy").

[27] *See* Nehf, *supra* note 2, at 30–31, 33–34.

[28] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2–3 (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf (the FTC discusses the prolific threat of identity theft, and notes that over three million complaints of appropriation were lodged from 2013 to 2015). *Compare* 11 U.S.C. § 107(c)(1)

A. Early Scholarship and Cases

Privacy can be viewed as a positive right to be protected or as a negative right enforced through a legal remedy.[29] Early scholarship included Warren and Brandeis's *The Right to Privacy* and William Prosser's *Privacy*, which illustrate the divergent perspectives.[30] Warren and Brandeis argued that privacy should be a right to be enjoyed,[31] while Prosser saw the issue as embodying four torts that offer remedies for privacy violations.[32] The distinction turns on whether the aim is to prevent harm or to provide redress.[33]

Privacy as a positive right involves the option of requesting government intervention and enforcement before a harm occurs.[34] Member states of the European Union provide the option of enforcing this positive right on unnecessary use of personal data,[35] while citizens retain negative rights to

(2012) ("The bankruptcy court, for cause, may protect an individual, with respects to the following types of information to the extent the court finds that disclosure of such information would create undue risk of identity theft or other unlawful injury . . ."); *and* 11 U.S.C. § 332 (2012); *and* 11 U.S.C. § 363 (2012); *and* 18 U.S.C. § 1028(d)(7) (2012); *and* FED. R. BANKR. P. 9037; *and* Bankruptcy Abuse Prevention and Consumer Protection (BAPCPA) Act of 2005, Pub. L. No. 109-8, §§ 231–34, 110 Stat. 23 (in each of the aforementioned laws, consumer privacy protections are intended to be protected ex-ante, to prevent appropriation) *with* RESTATEMENT (SECOND) OF TORTS, § 652A(2) (1979) ("The right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or (b) appropriation of the other's name or likeness, as stated in § 652C; or (c) unreasonable publicity given to the other's private life, as stated in § 652D; or (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.").

[29] *See* Nehf, *supra* note 2, at 5–6; Prosser, *supra* note 26; Charles Fried, *Privacy*, 77 YALE L.J. 475, 486–88 (1968); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 7–9 (1989).

[30] *Compare* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205–06, 213–20 (1890), *with* William L. Prosser, *supra* note 26.

[31] Warren & Brandeis, *supra* note 30, at 211 ("[N]ow that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.").

[32] Prosser, *supra* note 26 (establishing four torts for the invasion of privacy: "[i]ntrusion upon the plaintiff's . . . solitude, . . . public disclosure of embarrassing private facts about the plaintiff . . . publicity which places the plaintiff in a false light in the public eye[, and] [a]ppropriation . . . of the plaintiff's name or likeness").

[33] The different vantage points, and their corresponding effects on what is instituted, are most clearly illustrated by criminal law and the difference between utilitarian and retributive theories of justice. Namely, the difference lies in that the former seeks to deter future harm, while the latter seeks to punish. Both aim to address crime, albeit through distinctly different methods. *See, e.g.*, John Bronsteen, *Retribution's Role*, 84 IND. L.J. 1129, 1131–33 (2009); Gerard V. Bradley, *Retribution: The Central Aim of Punishment*, 27 HARV. J.L. & PUB. POL'Y 19, 30 (2003) ("[R]etribution attempts to restore social balance instead of seeking only to discourage similar criminal behavior.").

[34] The right to be forgotten, as asserted in Europe, is illustrative of this. *See* Press Release No 70/14, Court of Justice of the European Union, Judgment in Case C-131/12 (May 13, 2014), *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf ("[T]he Court holds that a fair balance should be sought in particular between that interest and the data subject's fundamental rights, in particular the right to privacy and the right to protection of personal data.").

[35] EUR. COMM'N, *Factsheet on the "Right to be Forgotten" Ruling* (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

remedies.[36] These comprehensive laws are a relatively new replacement to what had been a patchwork of legal treatments.[37]

United States privacy law still operates on an organically developed framework founded on negative rights.[38] Privacy violations are generally remedied through tort actions and, in limited circumstances, the law grants positive rights, such as the protection against search and seizure.[39] Advancing technology inspired legal developments through litigation as opposed to legislation.[40]

While technology spurred early privacy law, jurists' responses to technological changes lagged behind technological developments. Courts initially did not find protections for intrusions of privacy analogous to those that existed for physical intrusions, nor did they foresee how privacy threats would continue to mount. Brandeis, however, excelled where his peers failed, and his fear that "what is whispered in the closet shall be proclaimed from the house-tops" preceded decades of legal developments.[41]

In *Olmstead v. United States*, the Supreme Court faced the question of whether the warrantless wiretapping of a citizen's home violated the Fourth Amendment.[42] The majority held that there was no violation of constitutional protections because there was no seizure of physical effects nor physical invasion of the home.[43] Brandeis presciently dissented in *Olmstead*: "But 'time works changes, brings into existence new conditions and purposes.' Subtler and

---

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679**;** Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.., 2016 O.J. (L 119) 89, 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680.

[37] *See* Regulation (EU) 2016/679, *supra* note 36, at 89.

[38] From wiretapping in *Katz* to digital collection of children's information, privacy has developed as a response to stimulus. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353, 357–59 (1967); Fed. Press Release, Federal Trade Commission, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000) [hereinafter Toysmart Press Release], https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding.

[39] For an overview of privacy law, *see generally* Nehf, *supra* note 2, at 29–58.

[40] *See, e.g.*, Katz, 389 U.S. at 353, 357–59; Olmstead v. United States, 277 U.S. 438, 456–57, 464–66 (1928); Fed. Trade Comm'n v. Toysmart, 2000 U.S. Dist. LEXIS 21963, at *1 (D. Mass. 2000).

[41] *See* Warren & Brandeis, *supra* note 30, at 195.

[42] Olmstead, 277 U.S. at 455.

[43] *Id.* at 466.

more far-reaching means of invading privacy have now become available to the government."[44] Here, he saw what others did not: technology was outpacing the law.

After nearly four decades of failing to recognize non-physical invasions, the Court held in *Griswold v. Connecticut* that "the First Amendment has a penumbra where privacy is protected from governmental intrusion," which affirmed the right to privacy.[45] Two years later, in *Katz v. United States,* the Court removed physical intrusion as a requirement for an invasion of privacy.[46] History reflects the law's sluggish progression when compared to the alacrity with which technology advances. For example, in the forty years that the law had taken to recognize, in *Katz*, that wiretapping falls within the Fourth Amendment, televisions had become widespread and video recording equipment had become available for home use.[47] This disparate rate of the development of law and technology persists into the digital age of "[s]ubtler and more far-reaching means of invading privacy."[48] While Brandeis wrestled with wiretapping a private home, today, our information is tracked on a scale previously unimagined.[49] The digital age introduced a host of legal issues such as the distribution of consumer data as a bankruptcy asset.

B. FTC v. Toysmart

FTC v. Toysmart is the seminal case addressing consumer privacy policies and consumer data sold in bankruptcy.[50] Prior to its bankruptcy filing in 2000,

---

[44] *Id.* at 473.

[45] Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

[46] *See* Olmstead, 277 U.S. at 466; Katz, 389 U.S. at 353, 359 (wiretapping criminal acts in a public phone booth qualified as a search and seizure).

[47] *See* Olmstead, 277 U.S. 438; Katz, 389 U.S. 347; COBBETT STEINBERG, TV FACTS (1980) (prevalence of television sets in American households).

[48] Olmstead, 277 U.S. at 473. Comparing legal development and technology shows the disparity of pace. *See, e.g.*, Olmstead, 277 U.S. at 455, 466 (physical intrusion was required for illegal search and seizure, yet wiretapping already existed); Katz, 389 U.S. at 353, 359 (wiretapping was finally considered an invasion, but TV broadcasts were now common and home video technology had been released); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191 § 221, 110 Stat. 1936 (addressing the need to store private health information, but falling behind the widespread use of the internet); Gramm-Leach-Bliley Act, Pub. L. No. 106-102 §§ 501–27, 113 Stat. 1338 (1999) (conceiving notice and consent, but seemingly ignorant of the widespread use of the internet and growing cellular market); Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCA), Pub. L. No. 109-8, § 232, 110 Stat. 23; Fed. Trade Comm'n v. Toysmart, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000) (responding to the collection and distribution of consumer data from online customer accounts, without acknowledging the widespread collection of metadata and the ease of re-identification).

[49] Mark Mulcahy, *Big Data Statistics & Facts for 2017*, WATERFORD TECHNOLOGIES (Feb. 22, 2017), https://www.waterfordtechnologies.com/big-data-interesting-facts/.

[50] *See* Rich Letter, *supra* note 9; Vladeck Letter, *supra* note 8.

Toysmart.com advertised, promoted, and sold toys to adults and children.[51] The collected names, addresses, and shopping history of Toysmart customers were offered for sale in bankruptcy, contrary to the terms of the company's privacy policy.[52] Through their combined efforts, the FTC and the bankruptcy court confronted the unauthorized collection of children's data and resolved the issue of the sale of customer data contrary to the Toysmart.com privacy policy.[53]

Toysmart.com customers purchased goods under privacy policy terms that dictated "[p]ersonal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party."[54] Therefore, allowing the sale of this consumer information would seem to contravene the contractual obligations arising under the privacy policy.[55] FTC Commissioners Anthony and Thompson believed, however, that restricting how and to whom the information could be sold would address consumer privacy interests, maximize repayment to creditors, and provide a satisfactory compromise between those concerns.[56] Consumer privacy interests would be protected through data anonymization and creditors would be served by the sale of the data. Therefore, this perspective supported a looser interpretation of contract terms.

FTC Commissioner Swindle conceded that the proposed compromise was better than allowing a completely unrestricted sale of the information, but he ultimately dissented on grounds that the bankruptcy order should enforce the company's promise never to sell customer information to a third party.[57] In a footnote, he added that he would have supported the majority position if

---

[51] Toysmart Press Release, *supra* note 38.

[52] *Id.*

[53] *Id.; see also* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 (providing protection to children surfing the internet); *Toysmart.com Privacy Policy*, TOYSMART.COM, http:www.ftc.gov/os/2000/07/toyexh1.pdf ("Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party.").

[54] Toysmart Press Release, *supra* note 38; *Toysmart.com Privacy Policy*, *supra* note 53.

[55] Toysmart Press Release, *supra* note 38; *Toysmart Privacy Policy*, *supra* note 53*; see also* U.C.C. § 2-206 (amended 2002) (offer and acceptance in formation of contracts requires offer and acceptance); Stipulation and Order Establishing Conditions on Sale of Customer Information, No. 00-13995 (CJK) (D. Mass. Jul. 20, 2000), https://www.ftc.gov/sites/default/files/documents/cases/toysmartconsent.htm (ruling that Toysmart violated 15 U.S.C. § 45(a) (2012) "by disclosing, selling or offering for sale personal customer information, contrary to the terms of its privacy policy that personal information would never be disclosed to third parties").

[56] *See* Anthony Statement, *supra* note 8; Thompson Statement, *supra* note 8.

[57] Statement of Commissioner Orson Swindle, Toysmart.com, No. X00-0075, No. 00-13995 (CJK) (D. Mass. Jul. 21, 2000) [hereinafter Swindle Statement] ("Toysmart promised its customers that their personal information would never be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because 'never' really means never.").

customers had been given adequate notice and willingly consented to the terms presented in the bankruptcy order.[58] The FTC's decision thereby prioritized creditors' economic redress above consumers' privacy.[59] This set a precedent that allowed bankruptcy courts to alter privacy agreements in two ways: (1) privacy policies could still allow the transfer of consumer data to a third party, if it was done through estate distribution in bankruptcy, and (2) courts could now alter privacy contracts to bind parties to new terms or to new parties.

II. CURRENT LEGAL SOLUTIONS TO PRIVACY PROBLEMS

Congressional and regulatory oversight of consumer privacy began a few years after *Griswold* and *Katz* were decided in 1965 and 1967.[60] Laws such as the Fair Credit Reporting Act of 1970 (FCRA), the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Children's Online Privacy Protection Act of 1998 (COPPA), and the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA) each focus on different sectors of information.[61] Although the FTC has been delegated the authority to protect consumers and their privacy, these acts represent further legislative guidance. Here, Congress defined personal information differently for each sector, which in turn limits what the FTC can consider sensitive information that it is charged to protect.[62]

A. Privacy Laws

In 1970, Congress delegated authority to protect consumer privacy to the FTC through the FCRA.[63] This act was the first federal law regulating the use of

---

[58] *Id.* at n.1 ("If Toysmart had obtained the consent of its customers to a sale of the customer lists to a buyer that met the specific conditions spelled out in the Bankruptcy Order, I would have had no objection to the sale.").

[59] Toysmart Press Release, *supra* note 38.

[60] Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (recognizing that "Constitutional guarantees," including the Fifth Amendment, create a "zone of privacy" encompassing married couples' use of contraceptives); Katz v. United States, 389 U.S. 347, 353, 359 (1967) (holding that the Fifth Amendment protects against searches that invade reasonable expectations of privacy).

[61] The laws listed are not exhaustive but do provide an illustrative sample of legislative treatment. *See, e.g.*, Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (2012); Privacy Act of 1974, 5 U.S.C. § 552a (2012); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6505 (2012); Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, §§ 231–34, 110 Stat. 23.

[62] The FTC recognizes a consensus that data—such as that collected from children, financial transactions, health information, and social security numbers—comprises sensitive information, which should require notice of terms by the company and consent from the customer. PRIVACY REPORT, *supra* note 1, at 58–59.

[63] The FTC regulates consumer reporting agencies and limits the use of information collected, such as credit history and payment patterns, as well as demographic and identifying information. *See* Fair Credit

personal information by private businesses and it sought to promote the accuracy, fairness, and privacy of consumer information in the growing credit reporting industry.[64] By collecting large amounts of private data, credit reporting agencies became a powerful force in expanding credit availability and promoting economic efficiency.[65] However, to ensure accuracy and prevent abuse, the FTC required that consumers be notified and give consent before information is collected.[66] Although the act was pivotal in considering both consumer privacy and economic efficiency, it covered only a small sphere of consumer privacy. Subsequent legislation aimed to expand protection in other sectors of business while simultaneously promoting economic efficiency. In a rare instance of legal foresight, Congress safeguarded against deficiencies in future legislation by granting the FTC the authority to devise regulatory stop-gap measures.

The increasing rate at which government agencies were collecting, maintaining, and disseminating personal records prompted the Privacy Act of 1974.[67] Congress barred the communication of personal information to any person or agency without the express consent of the person involved, although exceptions were carved out for the operation of the government.[68] The Act was updated in an attempt to keep up with advancing technology, such as the 1988 and 1990 updates to address the growth of computer usage.[69] Having demonstrated its intent to safeguard privacy against government intrusion, Congress turned its attention to other areas of priority during the 1990s.

Congress passed HIPAA to combat abuse of Protected Health Information (PHI).[70] In 1995, an estimated 84.6 percent of the U.S. population was reportedly covered by some form of health insurance, which helped meet the demands of

---

Reporting Act (FCRA), 15 U.S.C. § 1681; FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT, AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 1 (July 2011), [hereinafter FTC STAFF REPORT], https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

64 *See* Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (2012).

65 *See* MARK FURLETTI, FED. RESERVE BANK OF PHILA., *An Overview and History of Credit Reporting* 4–6 (Jun. 2002), https://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2002/CreditReportingHistory_062002.pdf; Rowena Olegario, *Credit-Reporting Agencies: Their Historical Roots, Current Status, and Role in Market Development* 8–9 (World Bank, Working Paper No. 27825, 2001), http://siteresources.worldbank.org/INTWDRS/Resources/477365-1257315064764/2429_olegario.pdf.

66 FTC STAFF REPORT, *supra* note 63, at 2.

67 *See* Privacy Act of 1974, 5 U.S.C. § 552a (2012).

68 *Id*.

69 Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508, 104 Stat. 1388.

70 Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

the aging baby boomers.[71] As the number of participants in healthcare increased, so did the attempts to take advantage of them.[72] In response, the law's heavy regulatory scheme seemingly prioritized consumer privacy concerns over economic efficiency.[73] This trade-off may have been shortsighted, however, considering that National Healthcare Expenditure (NHE) accounted for 12.7 percent of Gross Domestic Product (GDP) in 1995, reaching $957.8 billion.[74] It then grew to approximately $3.3 trillion, accounting for 17.9 percent of U.S. GDP in 2016.[75]

HIPAA protects consumer privacy by placing strictures on how companies can store and transfer consumer data.[76] Since customers can trust that the transfer of data from one company to another will follow these more secure protocols, consumers may be less fearful about changing providers of insurance or healthcare, which bolsters market competition. Furthermore, HIPAA assigns both positive and negative rights to PHI.[77] It sets security standards to protect PHI as a positive right, and it enforces the negative right by punishing misuse, abuse, or lack of security.[78] Healthcare fraud and abuse cost an estimated $100 billion in 1995 and rose to $260 billion in 2012.[79] Here, the fact that 84.6 percent

---

[71] *Population Profile of the United States* 4, U.S. CENSUS BUREAU (1997), https://www.census.gov/prod/3/98pubs/p23-194.pdf.

[72] *Health Care Fraud Report*, U.S. DEPARTMENT OF JUSTICE 1–2 (Oct. 27, 1997), https://www.justice.gov/opa/us-department-justice-health-care-fraud-report.

[73] Meredith Kapushion, *Hungry Hungry HIPAA: When Privacy Regulations Go Too Far,* 31 FORDHAM URB. L.J. 1483, 1502 ("HIPAA's high costs, questionable benefits, and numerous economic, legal, and administrative consequences make a strong case for repeal.").

[74] Cathy A. Cowan & Bradley R. Braden, *Business Households and Government: Healthcare Spending, 1995*, 18 HEALTH CARE FIN. REV. 195, 196 (1997); CTRS. FOR MEDICARE & MEDICAID SERVS, NATIONAL HEALTH EXPENDITURES *2015*, HIGHLIGHTS, https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/downloads/highlights.pdf; *United States GDP Data from the World Economic Outlook Database*, INT'L MONETARY FUND (Oct. 2016), http://www.imf.org/external/pubs/ft/weo/2016/02/weodata/weorept.aspx?pr.x=25&pr.y=9&sy=2015&ey=2020&scsm=1&ssd=1&sort=country&ds=.&br=1&c=111&s=NGDPD%2CNGDPDPC%2CPPPGDP%2CPPPPC&grp=0&a=#download.

[75] Cowan, *supra* note 74; CTRS. FOR MEDICARE & MEDICAID SERVS, *supra* note 74; *United States GDP Data*, *supra* note 74.

[76] 45 C.F.R. § 164.530 (2012).

[77] *Id*.

[78] *Id*.

[79] COMM. ON GOV'T. REFORM AND OVERSIGHT, HEALTH CARE FRAUD: ALL PUBLIC AND PRIVATE PAYERS NEED FEDERAL CRIMINAL ANTI-FRAUD PROTECTIONS, H. R. REP. NO. 104-747 (1996) ("Health care fraud [is], by some estimates, a $100 billion problem."), https://www.congress.gov/congressional-report/104th-congress/house-report/747/1; Press Release, U.S. Attorney's Office for the Middle District of Louisiana, Medicare Fraud Strike Force Charges 107 Individuals for Approximately $452 Million in False Billing (May 2, 2012) ("The United States spends more than $2.5 trillion on health care annually and rough estimates indicate that anywhere from 3 to 10 percent of all health care expenditures are attributed to fraud"), https://archives.fbi.gov/archives/neworleans/press-releases/2012/medicare-fraud-strike-force-charges-107-individuals-for-approximately-452-million-in-false-billing.

of the U.S. population faced privacy threats, and nearly 12.7 percent of domestic GDP faced hundreds of billions in financial harm, add substantial support to the notion that pecuniary interests were at play in congressional intent.

In 1998, Congress passed COPPA to protect the privacy of children younger than 13.[80] Children faced increased marketing attention at home and in schools.[81] Congress was concerned about online advertising in the 1990s because the interactivity of the medium posed a new threat.[82] To mitigate the risk of harm, COPPA requires parental consent, establishes privacy policy standards, and site operation guidelines.[83] The FTC addresses any statutory gaps.[84] After market adoption in 2002, 90 percent of websites provided notice, but only approximately half properly handled the information collected.[85]

Here, congressional intent focused on protecting children's privacy and placed a lower priority on economic considerations than on parental control.[86] However, the act applies only to websites that direct their operations at children or websites that possess actual knowledge that the information collected belongs to children.[87] These measures are mostly ineffective since websites can either target children without collecting personal information or collect information from users who do not self-identify as children.[88] Although Congress intended

---

[80] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 (2012).

[81] Channel One gave schools free audiovisual equipment and services, which allowed it to advertise to millions of children for two minutes a day. *See* Drew Tiene, *Channel One: Good or Bad News for Our Schools?*, 50 CHANGING CURRICULUM 46, (May 1993). Billions of dollars were spent in the 1990s on marketing to children. JAMES MCNEAL, THE KIDS MARKET: MYTH AND REALITIES, 14–15 (1999).

[82] *See* Angela J. Campbell, *Ads2Kids.com: Should Government Regulate Advertising to Children on the World Wide Web?*, 33 GONZ. L. REV. 311, 325–27 (1997–1998) (discussing the myriad methods that advertisers used to target children at the time).

[83] 15 U.S.C. § 6501 (2012).

[84] *Id*. § 6505.

[85] FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 15 (Apr. 2002), https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf.

[86] 15 U.S.C. § 6502 (2012).

[87] Lauren A. Matecki, *Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era,* 5 NW. J.L. & SOC. POL'Y. 369, 387 (2010) ("These screening methods are technologically ineffective, as computer-savvy children often know how to circumvent these attempted roadblocks. The ease of age falsification leads to a situation where children may share personal information on a website that seeks to operate outside of COPPA restrictions because it—officially—doesn't allow underage users.").

[88] 15 U.S.C. §§ 6501, 6502(b)(1)(A) (" . . . require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child.").

to protect children's privacy, the law contains large gaps that FTC regulations have yet to address.[89]

In 1999, the Graham-Leach-Bliley Act (or "GLBA")[90] repealed restrictions of the Glass-Steagall Act,[91] thus permitting insurance and bank holding companies to merge and enabling the formation of Citigroup.[92] The GLBA's preamble states its purpose is "[t]o enhance the competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial services providers, and for other purposes," which clearly shows that economic interests governed legislative intent.[93] In addition to promoting the economy, however, the GLBA's anticipation of potential privacy harms, stemming from the creation of the first "universal" bank in America, created compliance standards for financial privacy, safeguards, and pretexting protections.[94] These privacy rules operate under notice and consent frameworks.[95]

Although Congress put some safeguards in place for consumer privacy, those protections failed to recognize the increased threat posed by a single entity holding so much data.[96] The Citigroup merger consolidated the insurance and financial records of millions of customers, which increased the risk of harm posed by a data breach. Economic concerns were certainly paramount, but the notice and consent provisions in the act demonstrate that Congress did not completely ignore consumer privacy concerns, even if it failed to properly protect them.

---

89 *See generally* Matecki, *supra* note 87.

90 15 U.S.C. §§ 6801–09 (2012); Federal Reserve History, *Financial Services Modernization Act of 1999, commonly called Gram-Leach-Bliley* (Nov. 12, 1999) ("This legislation, signed into law by President Bill Clinton in November 1999, repealed large parts of the Glass-Steagall Act, which had separated commercial and investment banking since 1933. This led to the creation of financial holding companies, over which the Fed was granted new supervisory powers"), https://www.federalreservehistory.org/essays/gramm_leach_bliley_act.

91 Act of Feb. 27, 1932, ch. 58, Pub. L. No. 72–44, 47 Stat. 56; Act of June 15, 1933, 6573–66. Glass-Steagall Act, ch. 88, Pub. L. No. 73-65, 48 Stat. 162 (1933) (providing for the safer and more effective use of bank assets).

92 *See* 15 U.S.C. §§ 6801–09 (2012) (enhancing competition in the financial services).

93 Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

94 *See* 15 U.S.C. § 6801(b) (2012) (financial privacy rule and safeguards rule); 15 U.S.C. §§ 6821(a)–(b) (2012) (pretexting protection). Merging Citicorp and Travelers resulted in a banking, securities, and insurance service. *See* Arthur E. Wilmarth, Jr., *Citigroup: A Case Study in Managerial and Regulatory Failures*, 47 IND. L. REV. 69, 70–71 (2014) ("[S]upporters of the merger hailed Citigroup as the first modern American 'universal bank' . . . . ").

95 *See* 15 U.S.C. § 6802 (2012).

96 *E.g.*, Tom Zeller, Jr., *Personal Data for 3.9 Million Lost in Transit,* N.Y. TIMES (Jun. 7, 2005), http://www.nytimes.com/2005/06/07/business/personal-data-for-39-million-lost-in-transit.html (the United Parcel Service had lost in transit a box of computer tapes containing information on 3.9 million customers for the consumer finance subsidiary of Citigroup) (hereinafter Zeller).

Despite the intent to promote economic efficiency, the FCRA, the Privacy Act of 1974, and HIPAA all managed to address consumer privacy interests, perhaps due to each Act's particular subject matter. Both the Privacy Act of 1974 and HIPAA specifically addressed consumer information, while the FCRA and GLBA addressed economic efficiency. The FCRA promoted economic efficiency by regulating credit reporting, while the GLBA promoted economic efficiency by allowing the consolidation of businesses and peripherally addressing data.[97]

BAPCPA amended the Code to address privacy concerns and system abuse.[98] The act added the presumption of abuse,[99] mandated two years between filings,[100] and required credit counseling to qualify for protection.[101] Privacy protections within BAPCPA addressed the treatment of PII[102] and created a consumer privacy ombudsman.[103]

Provisions in BAPCPA mirror the FTC and bankruptcy court's prerequisites to selling consumer data laid out in *Toysmart*.[104] The court in *Toysmart*, which stated that "in the absence of overruling federal law, [the decision] is to be determined by reference to state law,"[105] seemingly should have honored state

---

[97] *Privacy Act of 1974*, UNITED STATES DEPARTMENT OF JUSTICE (July 17, 2015), https://www.justice.gov/opcl/privacy-act-1974 (The act specifically references information gathered by federal agencies, the term "consumer" here is referencing the citizens who information is collected); *Summary of the HIPAA Security Rule*, UNITED STATES DEPARTMENT OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Mar. 18, 2018) (describing how HIPAA protects health information about actual persons); Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, 84 Stat. 1114, https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf (every instance of information gathering specifically addresses the growing need for standardized data collection and distribution for the changing infrastructure of 1970); Fed. Trade Comm'n, *Gramm-Leach-Bliley Act* (Sep. 4, 2015), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act ("The Gramm-Leach-Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data").

[98] *See* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 72.

[99] 11 U.S.C. § 707(b) (2012).

[100] *Id.* § 727.

[101] *Id*. § 109(h).

[102] *Id*. § 363 (b)(1).

[103] *Id*. § 332.

[104] Both *Toysmart* and BAPCPA allow for the transfer of consumer data contrary to prior obligations, with restrictions on alienation. *Compare* F.T.C. v. Toysmart.com, LLC, No. 00-CV-11341-RGS, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000), *with* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 72.

[105] Vanston Bondholders Protective Comm. v. Green, 329 U.S. 156, 161 (1946); *cf.* Swindle Statement, *supra* note 57.

contract law. Instead, the court held that debtors could sell consumer information under limitations similar to those later set forth in BAPCPA.[106] One of the limitations in both BAPCPA and *Toysmart* is the requirement that assets that contain personally or directly identifiable information—such as names, addresses, telephone numbers, or account numbers—be sold only to a qualified purchaser.[107]

The trial court in *Toysmart* required a qualified purchaser to (1) be in a related market, (2) continue to operate in the related market, and (3) agree to abide by the Toysmart.com privacy policy, unless customers gave affirmative consent before any material changes were made.[108] These requirements predated and inspired § 363(b)(1), which mirrors *Toysmart* by stating that PII can be sold only if the sale or lease is consistent with governing privacy policy terms, or if an appointed consumer privacy ombudsman approves the sale after notice and a hearing.[109] The consumer privacy ombudsman decides whether to approve the sale after considering the cost to consumer privacy, much as the FTC did in *Toysmart*.

BAPCPA clearly mirrors *Toysmart* in that consumer data can be sold only pursuant to governing privacy policies or if the consumer privacy ombudsman approves the sale after considering how it might affect consumer privacy. Congress relies on the FTC's regulatory authority to protect consumer privacy against threats from gaps in statutory protections.[110] Just as the FTC advised the court in *Toysmart*, BAPCPA intended the consumer privacy ombudsman to serve a similar advisory role.[111] Although BAPCPA contains measures to protect consumer privacy, technology has outpaced those protections.

B. Balancing Creditor Interests and Privacy

Bankruptcy courts and the FTC possess broad discretion over the sale of personal customer data in corporate bankruptcy filings,[112] both must consider

---

[106] *See* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 72.

[107] *Id*.

[108] F.T.C. v. Toysmart.com, LLC, No. 00-CV-11341-RGS, 2000 U.S. Dist. LEXIS 21963.

[109] 11 U.S.C. § 363(b) (2012); *see* 11 U.S.C. § 332 (2012).

[110] *See* 15 U.S.C. § 1681 (2012); *cf.* 15 U.S.C. § 6801 (2012). *See generally* 15 U.S.C. § 6501 (2012).

[111] 11 U.S.C. § 332 (2012) ("The consumer privacy ombudsman may appear and be heard at such hearing and shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B)").

[112] *See, e.g.*, *In re* Tweeter Home Ent. Grp., No. 07-10787 (PJW), 2007 Bankr. LEXIS 3418, (Bankr. D. Del. Oct. 2, 2007); Letter from David Vladeck, Dir., Fed. Trade Comm'n Bureau of Consumer Prot. to Peter

the circumstances of the sale, consumers' privacy interests, and the financial interests of creditors.[113] *Toysmart,* the seminal case in these matters, gave priority to creditor interests over consumer privacy concerns and allowed for the sale of information.[114] Bankruptcy courts and the FTC have since decided other cases by altering or ignoring contract terms, with varied methods and results.

In 2007, *In re Tweeter* displayed how a bankruptcy court's discretion can extend privacy policies beyond express limitations.[115] Tweeter Home Entertainment Group's online privacy policy specifically excluded retail and phone operations by stating that it covered "personal information collected via this Web site, and not through any other activities of Tweeter or its affiliates or business partners."[116] Since the proposed sale of all customer data collected would operate contrary to the privacy policy, 11 U.S.C. § 363(b)(1) required that a consumer privacy ombudsman be appointed to determine whether to allow the sale. The ombudsman and the FTC ignored the stated exclusions and recommended that Tweeter's policy extend to all three sales channels. The court agreed with these recommendations and sold all of Tweeter's PII. Thus, its decision outright altered contract terms to provide redress to creditors.[117]

In 2010, XY.com and XY Magazine filed for bankruptcy, and to prevent potential harm to customers, they were not allowed to sell PII.[118] During the case, concerns were raised about how customer information would be handled. Under § 363(b)(1), an ombudsman was appointed because the privacy policy would be violated by the proposed sale.[119] There, the FTC argued that customers had consented to have their information used only to operate XY.com and XY

Larson et al. (July 1, 2010), http://www.ftc.gov/os/closings/100712xy.pdf) [hereinafter Vladeck Letter to Larson]; *cf. In re* Borders Grp., 453 B.R. 459 (Bankr. S.D.N.Y. 2011).

113 11 U.S.C. § 363(b)(1)(B)(i) (2012).

114 Although the sale was allowed, it was not without objection. Commissioner Swindle said, "Toysmart promised its customers that their personal information would *never* be sold to a third party, but the Bankruptcy Order in fact would allow a sale to a third party. In my view, such a sale should not be permitted because 'never' really means never." *See* Swindle Statement, *supra* note 57.

115 *See In re* Tweeter Home Ent. Grp., No. 07-10787 (PJW), 2007 Bankr. LEXIS 3418 (Bankr. D. Del. Oct. 2, 2007).

116 *Id*.

117 *Id*.

118 Vladeck Letter to Larson, *supra* note 112.

119 CONSENT ORDER DIRECTING THE APPOINTMENT OF A CONSUMER PRIVACY OMBUDSMAN PURSUANT TO 11 U.S.C. § 332, Case No. 10-1443 (MBK), Doc. 77-1 (July 23, 2010), https://www.eff.org/files/consent_order_ombudsman.pdf; *see* 11 U.S.C. §§ 332, 363 (2012) (Section 332 explains the duties of an ombudsman, while § 363 delineates the appointment of an ombudsman).

Magazine. The purchaser countered that the sale should be allowed since he planned to restart both companies. [120]

In response, the FTC argued that "[d]ue to the nature of the information, the passage of time, and the closure of the magazine and website in 2007 and 2009, respectively, the continued use of the data may pose privacy risks not reasonably contemplated by subscribers . . . ."[121] The purchaser could not provide sufficient guarantees that information would be used with the same limitations as in XY's prior operations. In this case, the court placed greater value on consumer privacy concerns, since XY's customers could potentially face harm due to the sale of their data. As a result, unlike in *Toysmart* and *Tweeter*, consumer privacy concerns were given priority over creditor interests, and the court ordered the destruction of all of the PII.[122]

In 2011, the Borders bookstore chain was not allowed to sell its customers' personal information unless it honored its promise not to do so without their consent.[123] Borders' privacy policy, in 2006 and 2007, promised that it would disclose information to third parties only if the customer expressly consented to such disclosure.[124] Borders amended its policy on May 27, 2008, however, to allow the sale of consumer data in bankruptcy without express consent:

> Circumstances may arise where for strategic or other business reasons, Borders decides to sell, purchase, merge or otherwise reorganize its own or other businesses. Such a transaction may involve the disclosure of personal or other information to prospective or actual purchasers, or receiving it from sellers. It is Borders' practice to seek appropriate protection for information in these types of transactions. In the event that Borders or all of its assets are acquired in such a transaction, customer information would be one of the transferred assets.[125]

The FTC commissioner refused to accept the amended language applied to chapter 7 dissolutions and concluded that it should apply only to continuing operations, such as a merger or chapter 11 restructuring.[126] Since this was a chapter 7 filing, the privacy policy terms barred the sale, and 11 U.S.C.

---

120 11 U.S.C. §§ 332, 363 (2012)

121 *Id.*

122 *Id*.

123 *In re* Borders Grp., No. 11-10614 (MG), 2011 Bankr. LEXIS 4606 (U.S. Bankr. S.D.N.Y. Sept. 27, 2011).

124 Vladeck Letter to Baxter, *supra* note 8.

125 *See id.*

126 *See id.* ("We view this provision as applying to business transactions that would allow Borders to continue operating as a going concern and not to the dissolution of the company and piecemeal sale of assets in bankruptcy.").

§ 363(b)(1) again required the appointment of a consumer privacy ombudsman. The ombudsman and the FTC recommended that Borders seek express consent from customers before selling PII, and the court agreed. Customers who did not consent to the sale would have their PII purged.[127]

The FTC recognized that "bankruptcy may present special circumstances,"[128] and recommended the sale be allowed under BAPCPA conditions.[129] The bankruptcy court believed that Borders should be allowed to "marshal remaining assets for its creditors" by selling consumer information.[130] Barnes and Noble (B&N) was allowed to buy Borders' IP assets for $13.9 million so long as it conformed to the express consent policy.[131] This amount may seem significant, but B&N paid only about $0.35 for each consumer record purchased.[132]

In 2014, ConnectEDU's bankruptcy filing differentiated how PII would be sold in chapter 7 and chapter 11.[133] Unlike prior cases, where courts altered privacy policy terms to allow the sale of PII, here § 363(b)(1)(A) was strictly enforced, and ConnectEDU was not allowed to sell PII unless it complied with its privacy policy.[134] The FTC recommended that the court appoint a consumer

---

[127] Although it was not expressly defined in the letter from the FTC, the common usage of the word "purge," in this context, implied that the data would be destroyed similarly as in prior cases. *See* Vladeck Letter to Larson, *supra* note 112; *see also* F.T.C. v. Toysmart.com, LLC, No. 00-CV-11341-RGS, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000) (ordering the destruction of information collected from children).

[128] The FTC was referencing the unique circumstances of bankruptcy, where a company seeks either to reorganize or to liquidate assets to repay creditors. *See* Vladeck Letter to Baxter, *supra* note 8.

[129] The FTC would allow the sale if: (1) Borders agreed not to sell the customer information as a standalone asset; (2) buyer was engaged in substantially the same lines of business; (3) buyer expressly agreed to be bound by and adhere to the terms of Borders' privacy policy; and (4) buyer received affirmative consent from consumers for any changes to the privacy policy. Vladeck Letter to Baxter, *supra* note 8; *see* Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 231 (codifying the *Toysmart* standards).

[130] Vladeck Letter to Baxter, *supra* note 8, at 4.

[131] Mark S. Melodia & Paul J. Jaskot, *Barnes & Noble's Acquisition of Borders' Database on the Shelf?*, TECHNOLOGY L. DISPATCH (Sept. 23 2011), https://www.technologylawdispatch.com/2011/09/intellectual-property/barnes-nobles-acquisition-of-borders-database-on-the-shelf/ (as evidenced by the $13.9 million dollar price tag B&N agreed to pay for the IP assets).

[132] *See* Jeff Roberts, *Did B&N Pull a Fast One with Borders' Customer List?*, GIGAOM (Oct. 5, 2011, 11:48 AM), https://gigaom.com/2011/10/05/419-did-bn-pull-a-fast-one-with-borders-customer-list/ ("[i]n order to clinch its purchase of 40 million customer names from bankrupt Borders, Barnes & Noble made a series of promises to the court on steps it would take to protect the privacy of those customers.").

[133] *In re* ConnectEDU, Inc., No. 14-11238 (Bankr. S.D.N.Y. Apr. 28, 2014); Rich Letter, *supra* note 9.

[134] Rich Letter, *supra* note 9. The Commissioner incorrectly cited 11 U.S.C. § 353(b)(1)(A), which does not exist, instead of 11 U.S.C. § 363(b)(1)(A).

privacy ombudsman to ensure the protection of consumer privacy interests.[135] The court ordered ConnectEDU to provide users with proper notice and the opportunity to remove PII; otherwise the users' data would be destroyed. Ultimately, the court prevented the sale of PII because such sale would violate contract terms, and § 363(b)(1)(B)(ii) requires a "finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law."[136]

C. Technology, Data, and the Growing Threat

The law and data security have been outpaced not only by technology but also by the growing threat to privacy. Targeted services and information collection are not new to the digital age, but modern technology has certainly helped expand them.[137] Whereas efficient mailing systems facilitated direct marketing in the 1960's, today's age of big data allows for staggering breaches of email systems. One example of this would be in the Yahoo data breach of 2016, where 500 million individuals' records were exposed.[138] As the collection and use of consumer information continued to grow exponentially, the threat to consumer privacy soared, even prior to today's age of big data.[139]

In 1984, a single Sears, Roebuck & Company store failed to secure its password, which enabled hackers to steal 90 million credit histories from their

---

[135] However, current authority held by the ombudsman and common court treatment of these cases are insufficient to protect those privacy interests. Rich Letter, *supra* note 9; *see* 11 U.S.C. § 332 (2012) (if the sale goes against the privacy policy under a 11 U.S.C. § 363(b)(1)(A) review, then 11 U.S.C. § 332 requires the appointment of a consumer privacy ombudsman when the sale operates under 11 U.S.C. § 363(b)(1)(B)).

[136] 11 U.S.C. § 363(b)(1)(A) (2012).

[137] *See* Nehf, *supra* note 2 ("Direct marketing to individuals was an inefficient and comparatively costly business practice for most of the twentieth century . . . . Cyberspace technologies and the widespread use of the Internet profoundly affected the data collection business by the late 1990s.").

[138] *See id*. ("Sorting data by zip codes proved to be a rough but inexpensive way to reach certain demographic subgroups."); Gamio & Alcantara, *supra* note 4; *see also* Hayley Tsukayama, et al., *Yahoo Data Breach Casts 'Cloud' over Verizon Deal*, WASH. POST (Sept. 22, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/?utm_term=.28f2ef786a8f (comparing 32,000 records stolen in 2005 with the massive theft of 500 million records in 2016); Ernie Hayden, *Data Breach Protection Requires New Barriers*, TECHTARGET (May 2013), http://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers.barriers.

[139] *Identity Theft: Is There Another You?: Joint Hearing Before the Subcomm. on Telecomms.,* Trade & Consumer Prot. and the Subcomm. on Fin. & Hazardous Materials of the Comm. on Commerce H.R., 106th Cong. (1999). Although the entire report speaks to identity theft, a statement of note is made in discussing 15 U.S.C. § 1601: "[R]eports that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35,235 in 1992 to 522,922 in 1997, and that the Social Security Administration's Office of the Inspector General conducted 1,153 social security number misuse investigations in 1997, compared with 305 in 1996.".

archives, computers, or filing systems.[140] Although this was a massive data breach, it stemmed from the confluence of efforts by hackers and negligence by an employee.[141] On November 2, 1988, the Morris Worm was released. It crippled approximately ten percent of the 88,000 computers that were on the internet at the time and caused about $15 million in damage.[142] Note that the former was caused by user negligence and the latter was the result of a single person's creation.

In the 2000s, the GLBA[143] allowed for the formation of Citigroup, whose 2005 data breach was one in a series of examples that demonstrated the danger of increased data consolidation. Today's threat to privacy is the result of multiple factors coming together: the constant introduction of new technology; increased consumer adoption of technology and information systems; consumer trust in companies; and the lack of security against data breaches.

From 2005 to 2016, data breaches rose multiplicatively every few years, and the trend is unlikely to reverse without intervention.

---

[140] *See* Stuart Diamond, *Credit File Password is Stolen*, N.Y. TIMES (June 22, 1984), http://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html; Julianne Pepitone, *5 of the Biggest-Ever Credit Card Hacks*, CNNTECH (Jan. 12. 2014, 7:11 PM), http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/index.html.

[141] *See* Diamond, *supra* note 140; Pepitone, *supra* note 140.

[142] *See* Michelle Delio, *The Greatest Hacks of All Time*, WIRED (Feb. 6. 2001), https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/.

[143] 15 U.S.C. §§ 6801–6809 (2012).

Major Data Breaches (2005-2016)		
Year	**Entity**	**People Affected**
2005	Citigroup[144]	3.9 Million
2007	TJX Companies Inc.[145]	94 Million
2009	Heartland Payment Systems[146]	130 Million
2011	Sony PlayStation Network[147]	101 Million
2013	Target[148]	70 Million
2014	eBay[149]	145 Million
2015	US Voter Data[150]	191 Million
2016	Adult FriendFinder[151]	412 Million
2016	Yahoo[152]	1 Billion

As the chart above demonstrates, the increasing size and frequency of data breaches poses a problem for corporations. Although hardware is developing at a decreased pace, consumers are generating data at rapidly accelerating rates.[153] This is no anomaly. It simply shows that, as more consumers adopt new technologies or use information systems, the number of people generating data records increases in kind.[154] This trend contributed to an average increase in data generation by a factor of ten every two years since 1986[155] In 2013, 90 percent

144 *See* Zeller, *supra* note 96.

145 Pepitone, *supra* note 140.

146 Technically, the breach occurred over the course of multiple years, culminating in 2009. Andy Greenberg, *The Year of the Mega Data Breach*, FORBES (Nov. 24, 2009, 7:00 PM), https://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches.html#2d79ae04d038.

147 *See* Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN, https://digitalguardian.com/blog/history-data-breaches (last visited Jan. 27, 2017) (combining Sony's 2010 data breach of 77 million records with 2011's 24.6 million, for a total of 101 million).

148 *Id*.

149 Jim Finkle, *Hackers Raid eBay in Historic Breach, Access 145 Million Records*, REUTERS (May 21, 2014, 11:01 PM), https://uk.reuters.com/article/uk-ebay-password/hackers-raid-ebay-in-historic-breach-access-145-million-records-idUKKBN0E10ZL20140522.

150 Jim Finkle & Dustin Volz, *Database of 191 Million U.S. Voters Exposed on Internet*, REUTERS (Dec. 28, 2015, 7:22 PM), https://uk.reuters.com/article/us-usa-voters-breach/database-of-191-million-u-s-voters-exposed-on-internet-researcher-idUKKBN0UB1E020151229.

151 Andrea Peterson, *Adult FriendFinder Hit with One of the Biggest Data Breaches Ever, Report Says*, WASH. POST (Nov. 14, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/?utm_term=.121d3da61b4a.

152 Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

153 PETER HARSHA, *IT Research and Development Funding*, *in* CHASING MOORE'S LAW: INFORMATION TECHNOLOGY POLICY IN THE UNITED STATES 1, 22 (William Aspray ed., 2004); Åse Dragland, *Big Data – for Better or Worse*, SINTEF (May 22, 2013), https://www.sintef.no/en/latest-news/big-data-for-better-or-worse/.

154 *Id*.

155 Lucas Mearian, *Scientists calculate total data stores to date: 295+ exabytes*, COMPUTERWORLD (Feb. 14, 2011), https://www.computerworld.com/article/2513110/data-center/scientists-calculate-total-data-

of all data worldwide was shown to have been generated within the previous two years.[156] By December 31, 2016, Facebook's 1.86 billion monthly active users shared 216,302 videos per minute on Messenger.[157] Currently, Google processes 40,000 search queries every second, or 1.2 trillion searches per year.[158] As new users adopt technology, data generation increases at a disproportionately high rate, which produces alarming amounts of collected data.

Companies' success in properly harnessing the data they collect correlates with improved corporate performance. Some reports, in fact, suggest that a 10 percent increase in data accessibility can result in $65 million of additional net income for a typical Fortune 1000 company.[159] FTC reports predict that by 2020, there will be 50 billion internet-connected devices and that 90 percent of cars will have an internet connection.[160] The extensive and growing nature of data makes it essential for the law to keep pace. If the law fails to protect against technological threats today, as it did in *Olmstead*, the consequences will be drastic and may expose the intimate details of millions of individuals' lives.

D. Insufficient Means to an End

BAPCPA[161] and FTC regulatory goals may seek to protect consumer privacy, but the provisions, as drafted, provide insufficient protections for multiple reasons. First, bankruptcy courts may be applying state substantive law that should be trumped by federal law. Second, the scope of personally

---

stored-to-date--295--exabytes.html (humankind has stored 295 exabytes of data since 1986); Dragland, *supra* note 153; The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, EMC, https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm (last visited Mar. 18, 2018).

[156] Dragland, *supra* note 153; *accord Google Search Statistics*, INTERNET LIVE STATS, http://www.internetlivestats.com/google-search-statistics/#ref-2 (last visited Feb. 19, 2017, 6:25 PM).

[157] *Data Never Sleeps 4.0*, DOMO, https://www.domo.com/learn/data-never-sleeps-4-0 (last visited February 19, 2017).

[158] *Google Search Statistics*, *supra* note 156.

[159] Trips Reddy, *Creating a Future-Ready Company in 2017*, IBM WATSON (Dec. 21, 2016), https://www.ibm.com/blogs/watson/2016/12/creating-future-ready-company-2017-business-leaders-know/ (suggesting that a mere 10 percent increase in data accessibility will result in more than $65 million additional net income for a typical Fortune 1000 company). *Cf.* Ranjay Gulati, *Inside Best Buy's Customer-Centric Strategy*, HARV. BUS. REV. (Apr. 12, 2010), https://hbr.org/2010/04/inside-best-buys-customer-cent

[160] *Internet of Things*, FED. TRADE COMMISSION STAFF REP. i, 1 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[161] Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 23; *see Protecting Consumer Privacy*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy232 (the FTC has been the chief federal agency on privacy policy and enforcement since the 1970s).

identifiable information is too narrow. Last, qualified purchaser requirements contravene their intended purposes by limiting creditors' economic redress and increasing the likelihood that information will be re-identified.

1. Federal Discretion and Contracts

The sale of consumer data is customarily governed by bankruptcy courts who weigh the aims of bankruptcy against privacy concerns.[162] State law normally governs without federal override. BAPCPA, however, not only demonstrates the intent of Congress to allow bankruptcy courts to alter contract terms in privacy policies, but also grants them explicit authority to do so.[163] Some might argue that this authority contravenes contract law, but there are several reasons this is not the case.

The law has traditionally frowned upon restraints on the power of alienation, such as in the conveyance of property.[164] Companies offer goods to consumers in exchange for payment of the listed price and the collection of consumer data, and when customers buy from the company, they demonstrate acceptance of those terms.[165] When those privacy policies promise never to sell or lease the data, it is a restraint on alienation and thus a suspect contract term.[166]

However, consumer data is not identical to physical property. Turning instead to intellectual property law, importing concepts such as the first sale doctrine can provide analogies that further justify this override. In *Cuozzo Speed Techs., LLC v. Lee*, the Supreme Court analogized overturning a conviction based on the insufficiency of an indictment to disallowing *inter partes* review based on the "reasonable likelihood" of a party prevailing.[167] First sale doctrine states that once a copy of a copyrighted work is purchased from the copyright

---

[162] *Cf. In re* Tweeter Home Ent. Grp., No. 07-10787 (PJW), 2007 Bankr. LEXIS 3418 (Bankr. D. Del. Oct. 2, 2007); *see*, *e.g.*, Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 23; *In re* Borders Grp., No. 11-10614 (MG), 2011 Bankr. LEXIS 4606 (U.S. Bankr. S.D.N.Y. Sept. 27, 2011); *In re* RS Legacy Corp., No. 15-10197 (Bankr. D. Del. Feb. 5, 2015);

[163] *See* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, § 232, 119 Stat. 23.

[164] Although it does not strictly refer to information, the concepts of selling, leasing, or conveying consumer data are easy to analogize with property. *Cf.* Andrews v. Hall, 58 N.W.2d 201, 203 (Neb. 1953) ("It is the general rule that a grant or devise of real estate to a designated person in fee simple, with provisions therein that are inconsistent or repugnant thereto such as a restriction against the power to sell, mortgage, or otherwise encumber, conveys an absolute fee and such restrictions are void.").

[165] *Cf.* U.C.C. §§ 2-204, 2-205, 2-206, 2-207 (AM. LAW INST. & UNIF. LAW COMM'N 1977) (if a privacy policy is viewed as an additional term governing the collection of data, in addition to the offer and acceptance of the company's good or service).

[166] *See, e.g.*, Andrews, 58 N.W.2d at 202–03.

[167] Cuozzo Speed Techs., LLC. v. Lee, 136 S. Ct. 2131, 2153 n.7 (2016).

holder, the copyright holder cannot prevent the copy from being resold.[168] Here, just as the sale of a copyrighted work implicitly leads to the surrender of some rights, so may the sale of private consumer data allow privity to transfer from seller to purchaser in bankruptcies.[169]

Since BAPCPA expressly discusses the de-identification, transfer, and sale of consumer information sold in bankruptcy, similar reasoning can justify overriding state contract law.[170] Discretion has been given to bankruptcy courts to maximize a debtor's estate to repay creditors while protecting the privacy of consumers. The question, then, is whether that discretion is being properly employed to meet those goals.

2. De-identification and Lack of Security

Mirroring the law's failure to relinquish physical intrusion as a requirement for the invasion of privacy until *Katz*, the code's definition of PII is trapped in times past.[171] The Code's definition of PII is limited to a physical address and corresponding telephone number or a physical person's name, e-mail address, and social security number.[172]

> (A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes—
>
> (i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name;
>
> (ii) the geographical address of a physical place of residence of such individual;
>
> (iii) an electronic address (including an e-mail address) of such individual;
>
> (iv) a telephone number dedicated to contacting such individual at such physical place of residence;

---

168 17 U.S.C. § 109 (2012).

169 *See* Kirtsaeng v. Wiley, 568 U.S. 519, 526, 529 (2013) (addressing the question of transfer of rights of alienability in the purchase, sale, and resale of copyrighted works, as well as whether contract terms or first sale doctrine would apply if in contradiction with one another).

170 Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, §§ 231–32, 119 Stat. 23.

171 *See* Olmstead v. United States, 277 U.S. 438, 465–66 (1928) (holding that wiretapping conversations within someone's home was not an invasion of privacy, nor a violation of 4th or 5th Amendment protections); Katz v. United States, 389 U.S. 347 (1967) (recognizing nonphysical invasions of privacy).

172 11 U.S.C. § 101(41)(A) (2012). Note that this portion only applies if it is in connection with one of the above. As such, if someone has all of your data except for the things listed in § 101(41)(A), then it is not PII. That is why this Comment discusses how easy it is to identify someone without that data.

> (v) a social security account number issued to such individual; or
> (vi) the account number of a credit card issued to such individual; or
>
> (B) if identified in connection with 1 or more of the items of information specified in subparagraph (A)—
> (i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or
> (ii) any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically.[173]

This definition mainly addresses means of communicating with another person, but doesn't even begin to address the intimate details that can be gained by more modern data collection.[174] Consider that the code does not even peripherally address telephone metadata, such as text messages, numbers dialed, location tracking, or how long a conversation is held. Furthermore, the code covers only those telephone numbers that are "dedicated to contacting such individual at such physical place of residence."[175] This narrow scope arguably fails to include nearly half of United States households, as studies indicate that 49.3 percent of households use only wireless telephones.[176]

Furthermore, any argument that names, social security numbers, and e-mail addresses are protected by the current language neglects to consider that it might be entirely unnecessary to directly collect that information in the digital age. Metadata[177] labeled as "Customer Proprietary Network Information" is collected by telecommunications companies and "is densely interconnected, easily re-identifiable, and trivially gives rise to location, relationship, and sensitive inferences."[178] While PII may allow third parties to contact, locate, or potentially

---

173 *Id.*

174 *Id.*

175 *Id.*

176 Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey,* January–June 2016, NAT'L CTR. FOR HEALTH SCI. (Dec. 2016), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201612.pdf. To clarify the statistics, 49 percent of households are wireless-only, while 3.1 percent have no phone whatsoever, which would indicate that 52.4 percent of households don't have land lines. For the author's purposes, however, the only interesting number is the percentage of wireless-only households.

177 Metadata is generally defined as data that describes other data. This can take various forms including: image metadata regarding a picture's size, color profile, resolution, creation date, alteration date, software used to create it; web page metadata describing the keywords for search engines and scripts running; or text document data that describes the author, creation date, document size, and software used to create it.

178 Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata,* 113 PROC. NAT'L ACAD. SCI. (Apr. 2, 2015), http://www.pnas.org/content/113/20/5536.full.

defraud consumers, metadata can predict personal details.[179] One study was able to uncover private information, such as a subject's health conditions or even to infer whether someone owned an ArmaLite (AR) rifle, using only telephone metadata and linking data points to publicly available information, such as listed telephone numbers.[180] Current law provides customers with moderate protections from telemarketing, mass mailings, and e-mail spam, but does little to protect against identity theft or other invasions of privacy, such as revealing personal details through metadata.

One issue unaddressed by BAPCPA's requirement to de-identify PII is robocallers.[181] Robocallers auto-dial phone numbers using Voice Over Internet Protocol (VOIP) services to deliver pre-recorded messages.[182] Upon contacting a potential target, the system determines whether an individual is a desirable target before placing an operator on the phone.[183] The FTC reports that the agency has undertaken more than 100 enforcement actions against 600 companies and individuals responsible for billions of illegal calls.[184] Since robocallers auto-dial phone numbers until they reach a potential target, de-identifying PII is ineffective against this threat.[185] Recognizing this, the FTC has instituted more creative measures, such as crowdsourcing[186] security development to civic hackers.[187]

The fundamental flaw of de-identifying PII is that it attempts to minimize harm while retaining monetary value. Paul Ohm eloquently summarized the problem by stating, "[d]ata can be either useful or perfectly anonymous but never both."[188] Ohm proposed that de-identification comes at a greater cost to

---

179 *Id.*

180 *Id.*

181 *How Does A Robocall Work?,* FED. TRADE COMM'N https://www.consumer.ftc.gov/sites/default/files/pictures/0381-robocalls-infographic.png (last visited Feb. 3, 2017); *Robocalls,* FED. TRADE COMM'N, https://www.consumer.ftc.gov/features/feature-0025-robocalls (last visited 2/3/2017).

182 *How Does A Robocall Work? supra* note 181.

183 *Id.*

184 *Robocalls, supra* note 181.

185 *How Does A Robocall Work?, supra* note 181.

186 *Crowdsourcing*. MERIAM-WEBSTER ONLINE DICTIONARY (2018), https://www.merriam-webster.com/dictionary/crowdsourcing ("the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers").

187 *DetectaRobo*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/contests/detectarobo (last visited Feb. 3, 2017) ("As part of the National Day of Civic Hacking on June 6, 2015, the FTC challenged the tech-savvy public to DetectaRobo. Contestants analyzed call data to create algorithms that could predict which calls were likely robocalls.").

188 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010).

secure privacy, since re-identification continuously becomes easier and less expensive.[189]

Bankruptcy may provide a thin veil of protection for consumer privacy through de-identification, but these measures are easily pierced by linkage attacks.[190] Linkage attacks compare records in de-identified data sets with separate but related records to uniquely identify targets.[191] With a greater number of data points, the success of these attacks can reach near-certainty.[192] An early study used U.S. Census data to uniquely identify 61 to 87 percent of the United States population with only three data points: five-digit ZIP Code, gender, and date of birth.[193] The same study uniquely identified 18 percent of the U.S. population using only county, gender, and date of birth.[194] When the study combined gender and date of birth with city, town, or municipality in the linkage attack, 53 percent of the U.S. population could be uniquely identified.[195] The difference between the last two is explained by the fact that more people share a county of residence in common than a specific city, town, or municipality.[196] This demonstrates the inverse relationship between the number of people who share a data point and re-identification. In other words, as the number of people who share a data point increases, the utility of that data point for re-identification decreases.

Even seemingly innocuous information can re-identify an individual, given the presence of sufficient data points. In 2006, Netflix released de-identified records of 500,000 subscribers for a contest to suggest improvements for the Netflix movie recommendation service.[197] The data set was sparse and contained only movie ratings and dates, which Netflix believed made the information incapable of being re-identified.[198] Researchers uniquely identified 99 percent

---

189 *Id*.

190 Garinkel, *supra* note 3; *see* 11 U.S.C. §§ 107(c), 332, 363(b) (2012); 18 U.S.C. § 1028(d)(7) (2012); FED. R. BANKR. P. 9037; *see also* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), PL 109-8, §§ 231–32, 119 Stat. 23, 72–73.

191 Garinkel, *supra* note 3

192 *Id.*; Montjoye et al., *supra* note 3.

193 Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper, 2000), http://dataprivacylab.org/projects/identifiability/paper1.pdf.

194 *Id.*

195 *Id.*

196 *Id.*

197 Katie Hafner, *And If You Like the Movie, a Netflix Contest May Reward You Handsomely*, N.Y. TIMES (Oct. 2, 2006), http://www.nytimes.com/2006/10/02/technology/02netflix.html.

198 Arvin Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY 8 (2008), http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq.

of records that contained eight movie ratings and the dates they were reviewed.[199]

Alarmingly, the results remained accurate even if two of the reviews were falsified and the dates provided fell within a 14-day margin of error.[200] Using only two movie ratings and dates with a three-day margin of error allowed for 68 percent unique identification.[201] The research cross-referenced public IMDB ratings to bolster its records and further demonstrated that even something as trivial as movie preferences can reveal other, more personal details.[202] The Sweeney studies showed that the strength of a data point can greatly increase the success of a linkage attack. Yet, the Netflix study shows that, given a sufficient number of data points, linkage attacks can reach nearly 100 percent success rates regardless of the strength of each data point.

The amount of data collected and speed by which it can be processed renders de-identification as nothing more than a nuisance in the modern age.

3. Qualified Purchasers Are Better Linkers

Ever-growing data sets, the consolidation of data through bankruptcy, and linkage attacks present a combined threat to privacy unforeseen by existing legal treatments. This is made worse by the current "protection" measures requiring a qualified purchaser. The inefficacy of de-identifying PII would have been made evident when B&N purchased customer PII from Borders, but the court did not utilize de-identification and required an opportunity for customers to opt out instead.[203] Even if Borders customer PII had been de-identified, the Netflix experiment creates a reasonable expectation that each Borders customer could be re-identified by B&N.[204] Borders customer data that was de-identified could contain information such as age, ZIP Code of place of purchase, residence, book preferences, and date of purchase. B&N could cross-reference de-identified records with its own customer records and link the de-identified PII records to its existing customers. If any link failed, B&N could wait for further data points

---

[199] *Id.*

[200] *Id.*

[201] *Id.*

[202] *Id.*

[203] Nick Brown, *B&N Get Court's OK on $14 Million IP Sale*, REUTERS (Sep. 26, 2011), https://www.reuters.com/article/us-borders/borders-bn-get-courts-ok-on-14-million-ip-sale-idUSTRE78P5US20110926.

[204] Narayanan & Shmatikov, *supra* note 198.

as customers continued to buy books, or could wait for a Borders customer to buy his or her first book from B&N.

Since Borders cannot serve as a clear example, *RadioShack*'s disparate treatment of contract terms will help frame the issue further.[205] General Wireless purchased RadioShack and Apple customer information, but it was not allowed to purchase AT&T and Verizon customer data.[206] Since General Wireless and Sprint would be re-opening RadioShack stores together and would both compete with AT&T and Verizon in the mobile service market, the court was arguably preventing the acquisition of an unfair competitive advantage.[207] Apple, on the other hand, provides hardware and not mobile services, so Apple was unlikely to suffer unfair competition from the sale.[208] This decision reinforces bankruptcy courts' discretionary power and provides an example of de-identified data sets that were sold to someone with related data.

RadioShack customer data such as phone numbers, credit card information, social security numbers, dates of birth and other PII were de-identified to protect privacy, but this also adversely affected the value of the data set.[209] The problem is that the information still included the "where, when, and what," and likely also the "how," of an item's purchase. Thus, for each item purchased, there are at least three other data points. For example, if someone buys an iPhone from the new Sprint/General Wireless operation, then that person is almost certainly going to be re-identified. The inherent problem of the qualified purchaser requirement is that it greatly increases the likelihood of relatable data points, which defeats the purpose of data being de-identified in the first place.[210]

Requiring information be de-identified and sold only to qualified purchasers further devalues the already diminished bankruptcy sale price of consumer data. If contract terms are being ignored to provide redress to creditors, then bankruptcy courts should not work against the stated goal. In bankruptcy, Borders sold its intellectual property for $13.9 million, which equates to about

---

205 Rich Letter, *supra* note 9.

206 *See* Rich Letter, *supra* note 9; Salvatore, *supra* note 13.

207 *See* Rich Letter, *supra* note 9; Salvatore, *supra* note 13.

208 *See, e.g.*, APPLE, https://www.apple.com/ (last visited Mar. 18, 2018) (showing the site does not offer any mobile services to consumers).

209 *See* Suni Munshani, *RadioShack Customers Won this Round, We Still Need Better Data Privacy Guidelines,* VENTUREBEAT (May 25, 2015, 4:00 PM), http://venturebeat.com/2015/05/25/radioshack-customers-won-this-round-but-we-still-need-better-data-privacy-guarantees/.

210 Consider also that, in October 2016, the U.S. cellphone market share was 35 percent Samsung, 32 percent Apple, 14 percent LG, and 5 percent Motorola. *See* Lauren Guenveur, *LG Flourishes While Moto Struggles in the US,* KANTAR WORLDPANEL (Oct. 8, 2016), https://www.kantarworldpanel.com/global/News/LG-flourishes-while-Moto-struggles.

$0.29 per customer; RadioShack sold its intellectual property package for $26.2 million, or about $0.39 per customer.[211] Borders' top twenty unsecured creditors were collectively owed $241 million, which is over ten times what Borders collected by selling customer data.[212] RadioShack owed its top fifty creditors $373.9 million, which is seven times more than what it collected from selling its customer information.[213] Considering that neither RadioShack's nor Borders' customer data was sold as a stand-alone asset, these are likely inflated sale values.

These post-bankruptcy values are paltry when compared to the estimated $100 million Kroger earns annually by sharing data from its customers.[214] Although a solvent company's data is worth more than one in bankruptcy, that doesn't explain why Kroger earns thirty times more per year on a similar asset and does even less to explain how little data sells for in other circumstances.

Consumer data is rapidly generated, yet it is poorly secured. Both the rapid generation of consumer data and its poor security further limits consumer data values when they are treated as a commodity. Looking at general data values, as sold by brokers, sheds light on how little value can be placed on personal information. General information can be valued at as little as $0.0005 per person[215] while slightly more specialized information, such as PII of people receiving some healthcare treatment, can sell for up to $0.26 per person.[216] Knowing these values, we can infer that data values vary wildly depending on the buyer, seller, market, and content.

---

[211] Jenkins Simms, *Does $14 Million Worth of Email Addresses Cross the Privacy Line?,* CLIKZ (Oct. 6, 2011), https://www.clickz.com/does-14-million-worth-of-email-addresses-cross-the-privacy-line/49526/; Dawn McCarty, *RadioShack Name Goes to Standard General for $26.2 Million,* BLOOMBERG NEWS (May 13, 2015), https://www.bloomberg.com/news/articles/2015-05-13/standard-general-bid-of-26-5-million-wins-radioshack-brand.

[212] Judith Rosen, *Borders Bankruptcy Wends On,* PUBLISHERS WEEKLY (May 7, 2013), https://www.publishersweekly.com/pw/by-topic/industry-news/bookselling/article/57125-borders-bankruptcy-continues-to-cause-pain.html.

[213] *See* Danielle Abril, *RadioShack Bankruptcy: Here's How Much RadioShack Owes Top Creditors, Former Execs,* DALL. BUS. J., http://www.bizjournals.com/dallas/blog/techflash/2015/02/radioshack-bankruptcy-heres-how-much-radioshack.html (last updated Feb. 6, 2015); *see generally* Cases, PRIME CLERK (2018), https://cases.primeclerk.com/RadioShack/Home-ClaimInfo (table of creditor claims against RadioShack).

[214] Vipal Monga, *The Big Mystery: What's Big Data Really Worth?,* WALL ST. J. (Oct. 12, 2014), https://www.wsj.com/articles/whats-all-that-data-worth-1413157156 (estimating that Kroger receives $100 million per year from data sales).

[215] Emily Steel et al., *How Much is Your Personal Data Worth?,* FIN. TIMES (Jun. 12, 2013), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4Zqn3F16W.

[216] Emily Steel, *Companies Scramble for Consumer Data*, FIN. TIMES (Jun. 12, 2013), https://www.ft.com/content/f0b6edc0-d342-11e2-b3ff-00144feab7de.

4. Assets and Economics

Few concepts are as fundamental as supply and demand. Generally, as the number of buyers decreases, so does the demand for a product. The product's price will fall if a decrease in demand is not matched by a decrease in supply.[217] Consumer data follows the same principles, but the nature of its sale in bankruptcy may be better viewed as an auction rather than an open market.

Here, the willingness to pay is correlated to a few distinct qualities of the consumer data being sold. Some of these distinct qualities include number of data points, relevance to the purchaser's business, competition for the purchase, and the availability of substitutes. De-identification reduces the number of data points sold, which in turn decreases the value of a data set. Although the qualified purchaser requirement may increase the likelihood that a data set will be relevant to a potential buyer, it is self-evident that a buyer would be unlikely to purchase irrelevant data.

Instead, the qualified purchaser requirement reduces the number of competitors seeking the data set, which lowers demand and price. As established earlier, the availability of substitutes can be seen both as ever-increasing and finite, depending on the view. Since data is produced at such accelerated rates, there is always more data in the market, but the opposite argument would focus on the uniqueness of a data point. If each data point is unique, then a data set can potentially maintain value even if new data sets are created, or against the passage of time.

Consider Borders' customer information. The data set comprises the customer information of a consolidated book retail chain that was one of two major retailers in the business of brick-and-mortar bookselling. This data set shows the results of decisions made by Borders that are not shared by B&N, which can illustrate a variety of lessons on how to predict market outcomes based on certain inputs. If you combine it with the data already owned by B&N, you can then ascertain the total market effects of the two companies' divergent strategies.

Combining this data set with those of Best Buy and Circuit City would further allow a company to analyze the success and failure of companies in two markets with two principal retail chains. The problem with the qualified purchaser requirement is that, if a company is neither a bookseller nor an electronics retailer, it would not be allowed to purchase either data set.

---

[217] N. GREGORY MANKIW, PRINCIPLE OF MICROECONOMICS 71 (7th ed. 2014).

The qualified purchaser requirement seeks to make data safe and valuable, but instead reduces anonymity and stifles utility.[218] Imposing a limitation on who can purchase data does not increase value but, in fact, reduces value by limiting market demand, while doing nothing to increase safety. This decrease in consumer data value works against the principal aim of bankruptcy and decreases the incentive to protect privacy, since tort remedies are based on the harm suffered.

5. Reducing the Negative Right to Privacy

Torts are the common method for enforcing privacy. This places a great burden on consumers, because they must prove harm if they are to receive damages.[219] In theory, companies are supposed to protect consumer privacy both out of duty to customers and to avoid tort liability. If the law lowers consumer data values, it lowers the incentive for companies to provide security, the brunt of which is borne by the consumer. Since data values are so low, a company that fails to secure consumer data is unlikely to face any meaningful repercussions and thus has little incentive to operate otherwise.

In November 2014, Sony Pictures was hacked, which led to the breach of the social security numbers of over 47,000 celebrities and employees.[220] Sony spent $35 million to repair its financial and IT systems—an inconsequential sum compared to Sony's reported $331 million income, before taxes, in fiscal 2015.[221] The company's former director of information security openly admitted that investing $10 million to secure against $1 million in losses was not in the company's interests.[222] This mentality was especially evident in the manner in which the security systems were maintained. Sony's information sector

---

[218] Ohm, *supra* note 188.

[219] *See* Mark A. Geisfeld, *The Coherence of Compensation-Deterrence Theory in Tort Law*, 61 DEPAUL L. REV. 383, 394 (2011).

[220] Robert Hackett, *How Much Do Data Breaches Cost Big Companies? Shockingly Little,* FORTUNE (Mar. 27, 2015), http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/; Tim Hornyak, *Hack to Cost Sony $35 Million in IT Repairs,* NETWORK WORLD (Feb. 4, 2015), http://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html (describing the harm suffered by customers from data breaches at Sony, and how it pales in comparison to Sony's net income before taxes in the same calendar year).

[221] SONY, CONSOLIDATED FINANCIAL RESULTS FOR THE FISCAL YEAR ENDED MARCH 31, 2015 (Apr. 30, 2015), http://www.sony.net/SonyInfo/IR/library/fr/14q4_sony.pdf.

[222] Rex Santus, *Sony Pictures' Security Chief Once Thought Data Breaches Weren't a Big Deal,* MASHABLE (Dec. 5, 2014), http://mashable.com/2014/12/05/sony-hack-infosec-comments/#yMWplbHZdaqK ("'It's a valid business decision to accept the risk' said Jason Spaltro, who is now Sony Pictures' senior vice president of information security, in the interview. 'I will not invest $10 million to avoid a possible $1 million loss.'").

computers sat, logged in, in an unlocked room that was occasionally left unguarded.[223] When Guardians of Peace hacked Sony, the company was not just unprepared, it also failed to respond to the privacy threats with any sense of urgency.[224] Sony eventually strengthened its security, but only after the hacks resulted in the resignation of an executive and directly threatened Sony's ability to generate revenue. Movie stars, politicians, and many others were affected by leaked e-mails revealing controversial statements, which painted Sony in a negative light.[225] Sony is not the only company whose data has been compromised, nor is its breach cost to revenue ratio unique.

In 2013, hackers stole forty million Target customer credit card numbers and 70 million other customer records, such as e-mail addresses and phone numbers.[226] Target faced liability for a net total of $105 million after insurance reimbursements and tax deductions, accounting for 0.1 percent of Target's 2014 sales.[227] When an estimated fifty million Home Depot customer credit card and e-mail addresses were hacked, it cost Home Depot $28 million. This is less than 0.01 percent of its 2014 sales.[228] Since tort liability is the primary method to address privacy breaches, there is a need for change.

Sony's data breach cost more per record stolen than the Target or Home Depot breaches combined. The cause of this discrepancy can help determine the problem. Sony expected to pay $1063.83 per person, but the information was owned by wealthy individuals, those in possession of sensitive Sony information, or both.[229] Target paid $1.50 per person and Home Depot paid $0.56 per person, which is dwarfed by Sony's per-person costs. This difference is likely a combination of whose information was stolen as well as the fact that the Sony hack was politically motivated[230] rather than a simple data theft. In

---

223 Peter Elkind, *Inside the Hack of the Century, Part 1,* FORTUNE (Jun. 25, 2015), http://fortune.com/sony-hack-part-1/ ("Their Info Sec was empty, and all their screens were logged in. Basically the janitor can walk straight into their Info Sec department.").

224 *Id*. ("We are investigating an IT matter.").

225 *Id.* (Pascal's email exchanges)

226 Maggie McGrath, *Target Data Breach Spilled Info on as Many as 70 Million Customers*, FORBES (Jan. 10, 2014), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#cbe0d12e7954.

227 Hackett, *supra* note 220 (illustrating the inequity of burdens shared by consumers and companies in the face of data breaches and the loss of millions of customers' information).

228 *Id*. ("In the third quarter of fiscal 2014, [Home Depot] recorded $43 million of pretax expenses related to the Data Breach, partially offset by a $15 million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage, for pretax net expenses of $28 million.").

229 Hackett, *supra* note 220 (dividing $50 million estimated financial impact by the 47,000 affected individuals).

230 The hackers demanded that Sony withdraw a movie about a plot to assassinate the leader of North Korea. *See* Elkind, *supra* note 223.

2016, Yahoo's data breach became the largest in U.S. history, with 1.5 billion accounts exposed.[231] Although Yahoo lost $350 million from its sales price to Verizon, that loss translates to only $0.23 per customer record stolen.[232]

What makes the token cost to Home Depot and Target particularly egregious is that the Electronic Funds Transfer Act (EFTA) places a disproportionate burden on consumers to protect themselves when a company fails to secure data.[233] Under EFTA, a consumer who reports a card stolen within two days of activity is free from liability, but if the theft is reported after two days and before six months, the person can be liable for $50 to $500.[234] Customers can easily be liable for costs that are hundreds of times greater than when a company fails to protect data it has collected. Securing data costs time, money, and resources that companies are likely to spend elsewhere because they are liable for the smaller share of the cost when data is breached.

Current market interventions by the state seek to optimize economic efficiency, but arguably accomplish the opposite. Data sold in bankruptcy not only exacerbates privacy threats, but the sale contravenes bankruptcy's goal of providing redress to creditors.[235] Diminishing consumer data values in bankruptcy further reduce company liabilities for failing to secure data. Since consumers pay most of the cost of data breaches, it is important that the law promote privacy protections with greater efficacy to better serve the people.

De-identifying PII is a protection long outpaced by technology and only serves to lower consumer data values in bankruptcy. This treatment is neither useful to bankruptcy's goal of redress, nor is it an effective means of protecting privacy.

Qualified purchaser requirements place artificial limits on the number of buyers, which decreases competition and demand.[236] Since bankruptcy has limited influence on supply, decreases in demand will invariably decrease price.[237] Acting with the supply-demand curve in mind, bankruptcy courts can

---

231 Rodriguez, *supra* note 4 ("Yahoo announced that 500 million users' accounts had been exposed in a data breach. In December, the ailing internet company said another 1 billion accounts had been compromised in a separate attack—the largest in US history.").

232 *Id.* ("The pair agreed to slash $350 million off the original price tag.").

233 Hackett, *supra* note 220; 12 C.F.R. § 1005.6(b)(2)–(3) (2012).

234 12 C.F.R. § 1005.6(b)(2)–(3) (2012).

235 COLLIER, *supra* note 6.

236 *See, e.g.*, Rich Letter, *supra* note 9.

237 MANKIW, *supra* note 217 (discussing supply and demand).

better provide redress to creditors and also establish stronger incentives for companies to protect consumer privacy.

6. FTC as the Gap Filler

Acting FTC Chairman Ohlhausen recently wrote, "We have long defined sensitive information to include financial information, health information, Social Security Numbers, information about children, and precise geolocation information."[238] She further explains that the FTC now includes television viewing activity within the definition of sensitive information.[239] The FTC's justification is that the possession of television viewing activity can or is likely to cause a "substantial injury" under 14 U.S.C. § 45(n), but "substantial injury" in the context of consumer information requires clarification and reconsideration.[240]

Consumers face a greater threat of substantial injury as big data collects increasingly personal information, which reinforces the need for stronger data security.[241] Reports of dark web activity show what data is currently selling for and indicate that social media accounts and other communication account information sell for more than credit card information. The following chart lays out the going rates for different data sets.

Bank Credentials[242]	Credit Card[243]	E-mail Account[244]	Social Media[245]	Corp. E-mail Account[246]	IP Address[247]
$40 - 6% of balance	$7 - $30	$129	$129	$500	$90

[238] Statement of Acting Chairman Maureen K. Ohlhausen, *In re* Vizio, Inc., No. 1623024 (Feb. 6, 2017), https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhausen_2-6-17.pdf.

[239] *Id.*

[240] *Id.*; *see also* 14 U.S.C. § 45(n) (2012) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination").

[241] Caroline Humer & Jim Finke, *Your Medical Record is Worth More to Hackers than Your Credit Card,* REUTERS (Sep. 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

[242] *Underground Hacker Markets Annual Report*, SECUREWORKS (April 2016), https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report.

[243] *Id.*

[244] *Id.*

[245] *Id.*

[246] *Id.*

[247] *Id.*

Hackers seek personal information such as social media and e-mail accounts because identity is the foundation of financial transactions. The FCRA enabled the economy to use customer data and foresaw the need for protection even though the law has been inadequate in providing it. FTC regulations have worked to protect consumer privacy and have assisted bankruptcy courts in doing the same. This Comment proposes that bankruptcy better serve its own interests while assisting the FTC in its mission to protect consumers.

Bankruptcy courts are in the unique position to split the burden of protecting consumer privacy among the government, public, and companies. As Congress, the FTC, and the courts establish solutions, companies can be incentivized to respect consumer privacy as a right to be protected instead of a minimal cost to be ignored.

III. PROPOSED SOLUTIONS

If the law seeks to provide redress to creditors, then requiring a qualified purchaser and de-identifying consumer information works against that purpose. De-identification does not provide sufficient security, and qualified purchasers are more likely to circumvent the already weak protections. A limited pool of buyers decreases competition, which, in turn, decreases price. As the price of consumer data decreases, so does a company's liability if the data is breached. If consumer data sells for a greater value in bankruptcy, then the consumer can argue for a greater value when that data is breached, which strengthens companies' incentive to bolster security.

A. Bankruptcy Courts Should Use Their Discretion to Set Increased Minimum Liability for a Company's Failure to Secure Purchased Data

Asset distributions operate under constant state economic intervention from the moment the goods are made available to the state-regulated market.[248] These interventions are made necessary by the very nature of bankruptcy itself, since the discharge of debts often results in legally circumventing prior contractual obligations.[249] State interventions impose artificial limitations on market inputs, which directly affect market outcomes.

---

[248] *See* 11 U.S.C. § 726. (2012).

[249] Phillipe Aghion, Oliver Hart, & John Moore, *The Economics of Bankruptcy Reform*, *in* THE TRANSITION IN E. EUR., VOL. 2 (Jan. 1994), http://www.nber.org/chapters/c6727.

Bankruptcy courts should use their discretion to create more equitable alterations of contract terms. Currently, consumers are forced into privity of contract with new parties, often without consumer consent. Instead, to ensure that consumers are benefitting from the bargain or at least do not suffer from it, courts should require the purchaser of consumer data to accept increased liability for failing to secure consumer data. Establishing this liability can be done in two ways.

First, the court can calculate current market values for consumer data, not as it stands in bankruptcy, but as an asset in a living market. To establish the current market value of consumer data, courts should aggregate consumer data as expected values both in and out of bankruptcy. This will yield a value that is more commensurate with the actual market and allow for more accurate reflections of what values companies should place on security.

Expected values are predicted values of a variable, calculated as the sum of all possible values each multiplied by the probability of its occurrence.[250] Here, the court would aggregate an expected value by using four variables: (1) the value of the consumer data before bankruptcy, (2) the probability of surviving bankruptcy, (3) the value of the consumer data in bankruptcy, and (4) the probability of bankruptcy liquidation. Taking the product of the value of multiplying the value of the data before bankruptcy by the probability of the company surviving bankruptcy produces the probable value of the data outside of bankruptcy. Multiplying the value of data in bankruptcy and the probability of bankruptcy resulting in liquidation then produces the value of data in bankruptcy.

The value of consumer data before bankruptcy can be found by pricing similar consumer data available on the market. The court would use prior cases or prices offered to price the value of consumer data in bankruptcy in the current case. Probability of survival or liquidation could use prior bankruptcy cases with similar circumstances or other uses of discretion. Second, courts should calculate the average cost of consumer data breaches borne by the consumer and the government. In other words, aggregate the direct and incidental financial losses incurred from a data breach, such as the cost of paying for fraudulent charges, increased interest rates, decreased credit scores, and cost to investigate and combat fraud to find the value of the data. Once the aggregate harm is

[250] One example of this concept is the Learned Hand Formula used as a calculus of negligence. Judge Learned Hand proposed that negligence can be proven where the burden of preventing a harm is outweighed by the probability of the harm multiplied by the magnitude of the harm. *See* United States v. Carroll Towing Co., 159 F.2d 169 (2d. Cir. 1947).

established, the burden should be distributed among the negligent parties based on comparative fault.[251]

Combining these two calculations, a qualified purchaser can choose to accept a base amount of financial liability based on these values. If accepted, the company would then have to consider the cost of a guaranteed data breach against a calculated cost of security. For example, if a company totally fails to secure its data, then one can assume that a breach is guaranteed. Say that breach would cause the company to face $1 million liability. This incentivizes the company to spend no more than $1 million on protecting its data.

Now, take those same facts but add data security to the equation. The company knows that spending money on security will decrease the likelihood of a breach. Therefore, the company would be incentivized to conduct a cost-benefit analysis to determine how much money to spend on security. Assume that the company decides to spend $500,000 on security and estimates that this will reduce the chance of breach to 25 percent. In the current example, the company still incurs a risk of breach occurring but has now balanced that risk against the potential reward. By spending $500,000 on security, the company would have a 75 percent chance of incurring a $500,000 discount from the initial $1 million liability, but also has a 25 percent chance of incurring a liability of $1.5 million. These numbers would actually be smaller because it is intuitive

[251] To illustrate this, imagine a company has a 30 percent probability of successfully executing a chapter 11 plan and it possesses data on one million customers that is worth an aggregate market value of fifteen million. The value of the data would then be an estimated 4.5 million dollars, or $4.50 per customer. If that same company then has a 70 percent probability of being forced to liquidate through chapter 7 bankruptcy and the data will likely sell for half a million dollars, then the value of the data in bankruptcy would be $350,000 dollars or $0.35 per customer. If this were further aggregated by weighing each value, then the expected value of the data would be the product of the value in bankruptcy multiplied by the likelihood of liquidation added to the likelihood of surviving bankruptcy multiplied by the value of the data before bankruptcy. Here, that would result in a non-bankruptcy value of 1.35 million dollars and a bankruptcy value of $245,000 dollars resulting in an expected value of $1.595 million dollars. To calculate this number, the court simply looks to prior incidents. If a similar company suffered a breach and one hundred thousand consumers suffered an average loss of four hundred dollars, the consumer burden would be forty million dollars. If the government spent two million dollars combatting that breach and investigating the matter, then the government burden is two million dollars. That would be an aggregate of forty-two million dollars of harm. If eighty percent of consumers were found liable for half the loss due to improper security on their part, then that harm could be lowered to sixteen million for consumer harms and two million for government harms totaling eighteen million in aggregate harm. To prevent burdening companies with onerous penalties, that value would then be calculated using the Learned Hand Formula to establish duty. Calculate the likelihood of a data breach, multiply it by the aggregate harm, and then compare to the costs of securing the data. Instead of holding the company liable for all, the court can choose to discount the cost of securing data. Thus, in the above example, if the harm is $240 per consumer and the company spent $225 per consumer to prevent a breach, then the result would be $15 per consumer. The court could then require the company purchasing the data to accept a minimum liability of $15 per consumer record.

that if a company spends money on security, then a breach would result in less than 100 percent of the data being stolen, which means the liability would be lower.

In conclusion, the company's risk profile would determine how it conducts its cost-benefit analysis, which would influence how much money it chose to spend on security. As a general rule, if the damages a company would incur increases, so does the amount that is cost-effective to secure against those damages.

B. Bankruptcy Courts Should Redefine What Constitutes Qualified Purchasers and What They May Purchase

If the bankruptcy court redefines the qualified purchaser requirement, the pool of potential buyers will increase. This, in turn, should increase what companies pay for consumer data because there will be increased competition among prospective buyers. The threat of a purchaser abusing the data it acquires can be mitigated by setting liability minimums that elevate the company's risk calculations. The qualified purchaser requirement is supposed to limit the sale of consumer data to only those who seek the data for good faith reasons. If a company is not a qualified purchaser under the current framework, then it can demonstrate good faith by accepting increased liability.

Again, the bankruptcy court can use its discretion to set a limited increase in liability value for a "qualified purchaser," and a greater increased liability value for anyone who does not qualify for a discounted rate.[252]

C. Bankruptcy Courts Should Order Unsold Data Destroyed

If data is not sold in bankruptcy distributions under this system, then it demonstrates the data's lack of value or that no buyer is willing to accept the burden of securing the data. In either circumstance, the destruction of data serves the dual purposes of decreasing supply to increase the value of other data and of preventing the harm that would occur if an irresponsible buyer were to acquire the data.

If bankruptcy courts were to set increased minimum liability values for failure to prevent a breach of consumer data sold in bankruptcy, companies would have greater incentive to secure data and increase data values. These increased values would strengthen incentives to protect consumer privacy by

[252] Using the prior example, the value could be set between $15 and $240 per consumer record.

increasing the amount that companies pay for consumer data—both before and after bankruptcy filings. This circular relationship would see data security and values rise and would serve to increase redress to creditors while simultaneously increasing consumer privacy protections. In turn, it would raise awareness of consumer privacy, since there would now be a financial interest in protecting these rights.

CONCLUSION

Current legislative treatment aims to increase security and maximize redress. This treatment limits who may purchase data and attempts to increase security through anonymization. These efforts are meant to allow for private data assets to increase redress to creditors, but by compromising both, consumers are left without adequate privacy protections and the data sold is often undervalued. To combat this inefficiency, bankruptcy judges should use their discretion to increase the amount of redress to creditors while ensuring greater protections for consumer privacy.

By implementing a minimum liability value for failing to protect these assets, companies have an increased incentive to secure that data. The subsequent increase in security investment will affect the data's market value before bankruptcy, which in turn will increase its value in bankruptcy. As the liability for data breaches increases, so will investment and the end result will increase the security of consumer privacy and the redress provided to creditors when data is sold in bankruptcy.

DANIEL BRIAN TAN*

* Notes and Comments Editor, *Emory Bankruptcy Developments Journal*; J.D., Emory University School of Law (2018); B.A., Tulane University (2010). First, I want thank Nicole Morris for her guidance as my faculty advisor and being an integral part of my Emory Law experience. Second, my thanks to Vincent Comito and David Patton for their boundless will to debate ideas. Finally, I am grateful to the *EBDJ* staff and editors for two immensely rewarding years; my family for providing the foundations upon which my life is built; and my friends and colleagues who inspire me to continue building every day.